12-16-2019 1:00 PM

Resignation or Resistance? Examining the Digital Privacy Attitudes and Behaviours of East Yorkers

Kaitlyn Cavacas
The University of Western Ontario

Supervisor
Quan-Haase, Anabel
The University of Western Ontario

Graduate Program in Sociology
A thesis submitted in partial fulfillment of the requirements for the degree in Master of Arts

Abstract

Digital technologies have become enmeshed in everyday life causing the public to become exposed to potential privacy risks through data collection and aggregation practices. Further, the upsurge in use of social networking platforms has also created opportunities for privacy violations through institutional and social surveillance. Employing a qualitative thematic analysis, this study explores how adults (*N*=101) living in East York, Toronto, navigate privacy through their use of the internet and digital services. Participants expressed feelings of mistrust, loss of control, resignation, and perceived self-unimportance with regards to their digital data. Importantly, others noted their desire and attempts to gain agency when using online services. This study provides support for the rich and developing body of literature on the sociology of resignation; as such, it challenges the notion that digital users are unconcerned about their data online and argues for a re-evaluation of the "informed" and "empowered" actor metaphor at the heart of the privacy paradox debate.

Summary for Lay Audience

With the increased use of digital services and the internet becoming an ever-present phenomenon, concerns have emerged around privacy as related to digital data collection and use of personal data. This study investigates the privacy-related attitudes and behaviours of individuals living in the neighbourhood of East York, Toronto. Results reveal that individuals experienced feelings of loss of control in their use of digital services, and some viewed their digital data as being unimportant or uninteresting. Furthermore, respondents expressed experiencing mistrust towards various sources including other users online, corporations, the government and technological services. Despite the limitations faced in using digital services, users noted their efforts to gain control and exert agency over their personal data. This study supports the emerging literature on the sociology of digital resignation and argues for its inclusion as a theoretical model for understanding how users manage digital and online privacy.

Keywords

digital privacy, networked privacy, surveillance, social media, privacy paradox, resignation, East York studies

Acknowledgments

Firstly, I would like to thank my thesis supervisor, Dr. Anabel Quan-Haase. From the start of my project you have been encouraging and supportive which has allowed me to passionately hone in on my topic. Despite my changing ideas and theoretical direction you remained confident in my abilities, always providing a source of reassurance when needed. I am incredibly grateful for your mentorship. Your patience, unwavering kindness, attentiveness and thoroughness provided me with invaluable support throughout this journey and for this I am eternally grateful.

Secondly, I would like to thank Molly Harper. Your efforts in assisting with coding and editing have been incredibly helpful. This thesis would not be the same without your contributions. Your passion for bullying and youth shine a light on how incredibly kind and considerate you are and I thank you again for your work on this project.

Thirdly, I would like to thank the members of my defense committee, Dr. Michael Gardiner, Dr. Scott Schaffer, and Alison Hearn. Thank you for your input and time, it is greatly appreciated.

To my family, you mean everything to me. Your endless support throughout my life has provided me with the reassurance needed to pursue my passions. To my parents, your humility and open hearts have impacted the person I am today and I am endlessly grateful to have both of you as models of love in my life.

Finally, this thesis received financial support from the Social Science and Humanities Research Council of Canada (Grant Number: SSHRC 435-2015-1444). I am grateful to those who have advised and helped, especially those who transcribed and coded the interviews, as well as Barry Wellman, Christian Beermann, Brent Berry, Isioma Elueze, and Maria Kicevski. Most of all, I owe immense gratitude to the residents of East York who welcomed us into their homes.

Table of Contents

List of Figures

List of Appendices

Chapter 1

1 Introduction

Digital technology has become integrated into dominant institutions shaping the way individuals interact with the world around them. Major spheres that direct social and individual life —work, education, and social relationships— have irrevocably been altered due to transformations in technology. What has been particularly transformative of the way the digital has shifted modern experience is how it has changed the way we do ordinary things. The way we cook, eat, play, write, read, shop, talk, and travel have all been impacted. Digital technologies have offered more convenient avenues for achieving the outcomes we want and for this, we pay a price. Individual movements and interactions are now tracked through personalized media, namely media technologies that are used by individuals (Chayko, 2016). Further, surveillance cameras now capture conversations and actions that occur in public spaces making the experience of being watched an ever-present reality. Digital technology is intrinsic to practices of surveillance and has enabled governments and corporations to track, gather and sell personal data (Chayko, 2016). Some citizens feel their rights to privacy have been encroached upon, leading to concerns regarding data collection and aggregation practices. Indeed, a 2014 survey found that 80% of Americans were concerned about advertisers and businesses accessing the data they share on social media platforms and 64% were in agreement regarding the need of government to regulate advertisers (Madden, 2014). Further, a 2017 survey alarmingly found that of those who participated in the questionnaire (1,040 adults), roughly half did not trust the federal government or social media sites to protect their data (Smith, 2017).

Despite growing concern over the ways in which corporate and government entities handle data, digital users continue to provide information online, opening up opportunities for their data to be breached and compromised. This discrepancy between expressed concern over privacy and a lack of behaviour directed at protecting such privacy has been referred to as the 'privacy paradox' (Barnes, 2006; Kokolakis, 2017; Young & Quan-Haase, 2013; Hargittai & Marwick, 2016). This theory suggests that digital users who provide personal information online do so based on having assessed the

opportunities and consequences that can result from disclosure. It views privacy as a choice between "involvement in (or isolation from) various social and economic communities" which in turn positions the act of disclosure as a strategic decision made by rational consumers (Turow, 2017, p. 233). It paints a picture of the digital user as being an informed consumer who is aware of the risks to their data should they choose to disclose, thereby classifying the act of disclosing as an autonomous decision based on a calculative assessment of the pertinent information involved (Hoofnagle & Urban, 2014). The behaviour of digital users is viewed as paradoxical in that they express wanting privacy but seem to illogically disregard this preference through their disuse of privacy protective behaviours. Recent research has challenged this portrait of the informed and autonomous consumer and has argued for a re-evaluation of the digital user at the center of the privacy paradox debate (see Draper, 2017; Draper & Turow, 2019).

The sociology of digital resignation is a theory that provides a new framework for understanding the problem of privacy and how it is managed in digital contexts today. This theory argues that individuals provide personal information online because they have become resigned to the reality of limited control; i.e., they have become resigned to the inevitabilities that result from lack of control often experienced in digital spaces (Draper, 2016). Although users deeply care about their privacy and express wanting control over their information online, they feel unable to protect it. From this perspective, the act of disclosing information online for one who is concerned about privacy is not paradoxical; to the contrary it is quite sensible indeed. In believing that they cannot exert real influence or change to the ways in which their digital data is managed, users become resigned to the risks associated with digital engagement in order to remain connected despite their pressing concerns.

With consumer surveillance growing more sophisticated and pervasive as digital technologies are steadily integrated into people's everyday lives, the prospect of remaining anonymous or disengaged from digital technology has become unrealistic. Opting out from use of digital services and technologies can have social and economic consequences for some digital users, leaving them feeling compelled to remain digitally engaged (Hargittai & Marwick, 2016). Adding to this, avoiding use of digital technology does not necessarily guarantee one is free from possessing a digital presence (Lawrence

Öqvist, 2009). Due to the networked nature of our digital society people can post images, videos, and posts about another, leaving that person vulnerable to the online activity of others. Similarly, use of technology for basic and mundane actions (e.g., browsing the internet, purchasing items online and watching videos online, etc.) is tracked through cookies that companies then use to understand consumer behaviour (Lupton, 2015). This makes complete avoidance of surveillance virtually impossible. In realizing this, and the lack of control that accompanies digital engagement, users opt to use digital services and disclose personal information online because they believe that risks to their personal information are inevitable and unavoidable (Turow, 2017).

This theory also argues that the digital user is not sufficiently aware of the risks involved with disclosure of information and often lacks the basic knowledge needed to make informed cost-benefit decisions (Turow, Hennessy & Draper, 2015; Turow, 2003). This lack of knowledge contributes to one's willingness to provide information online and contradicts the *informed consumer* put forth in the privacy paradox. Previous research has shown that individuals with increased knowledge of data collection and surveillance practices on behalf of government and corporate sources are more concerned about privacy issues than those with less knowledge (Hoofnagle & Urban 2014). Ironically however, those with increased knowledge about data collection and its uses for marketing purposes are more likely to be resigned towards practices of privacy protection (Turow, Hennessy & Draper, 2015). They believe that they cannot seriously change government or business policy, which if they were permitted, would allow them to manage how their personal information is used. Further, some users feel swept up in the 'data-gathering marketing system' (Turow *et al.*, 2015) in which users engage unintentionally and intentionally in economic and social processes for positive gain (e.g. social connection through Facebook, low prices through membership in loyalty programs, etc.). The purpose of this paper is to illuminate the privacy concerns East Yorkers have with regard to their digital data, and how they manage these feelings. Particular attention will be paid to the unique privacy protection strategies that study respondents employ and their corresponding conceptions regarding the utility of these practices. The objective of this study is twofold: first, to provide an insightful analysis of East Yorkers and their views on digital privacy; and second, to understand how East Yorkers manage their privacy

concerns. In an effort to understand respondents' sense of agency and control within digital spaces, attitudes relating to resignation will be noted. In order to explore the theory of digital resignation and its applicability in different geographic regions, the presence of attitudes corresponding with a position of resignation will be analyzed in an effort to illuminate the conditions that incite feelings of resignation.

In the following pages I aim to shed light on the sociology of digital resignation and its relevance as a model for evaluating privacy attitudes and behaviours within a digital context. In Chapter 2, I review the literature and provide a detailed discussion of the theoretical foundation forming my approach. In this section, I address the role of surveillance in North American society and how it is markedly different from previous periods. I examine the theory of 'surveillance realism' (Dencik & Cable, 2017) and its connection to the sociology of digital resignation. Finally, I address the need for use of resignation as a model in discussions surrounding the privacy paradox debate. In Chapter 3, I present my research methodology. More specifically, this section details the demographics of the sample, the interview structure and topics, the internet experiences of study participants and an in-depth discussion on the process comprising my analysis of the data. In Chapter 4, I outline the main themes that resulted from analysis of the data: mistrust, perceived self-unimportance, loss of control, agency, and resignation. I then address the relevance and use of employing digital resignation as a theoretical model for understanding how people navigate privacy-related issues within a digital context. Finally, in Chapter 5 I discuss the above themes at greater length and explain how they connect to the theoretical framework outlined in Chapter 2. I also address the limitations and contributions of the current study as well as recommended directions for future research before concluding.

Before moving into the next section the main terms used throughout this paper will be defined in order to ensure clarification of the meaning of the words used is provided from the outset. Important to note here are the challenges associated with conceptualization of these terms. First, technology is rapidly evolving, which presents difficulties in establishing clear boundaries around terms such as the internet and social media. Second, many of the technologies discussed in this paper provide similar uses to other technology, introducing challenges in distinguishing the purpose and capabilities

characteristic of each. For instance, social media services facilitate maintenance of social networks, enabling people to communicate; yet this service is also provided by the telephone, which poses the question whether the telephone should be considered social media (Obar & Wildman, 2015).

With these important considerations in mind I will begin by providing a definition of the internet. Janet Abbate has suggested that the internet be understood as dynamic and based on a myriad of cultural manifestations (2017). She maintains that there is no one sufficient definition of the internet but rather multiple meanings that are connected to the term as a result of the content and boundaries that shape its definition. She argues that the internet can be represented by three features: first, it is technology; second, it serves as a space for content and sociality; and third, it provides a locally situated experience (Abbate, 2017). It is technology because it serves as infrastructure that is used as a channel for transmitting data. It is a space for content and social interaction through applications and services— social media, shopping, reading, banking and gaming— that are enabled through the technology. Finally, it represents a locally situated experience in that users "experience the internet through specific locally situated machines, programs, service providers and cultures" (Abbate, 2017, p. 11). Viewing the internet as locally situated acknowledges that users experience in using the internet is unique to their political environment, social position and personal capabilities (Abbate, 2017).

Frequently mentioned throughout this paper are the terms digital service and digital application. A digital service is a service that is obtained through a digital transaction which is made available by the infrastructure of the internet (Hevner & Chatterjee, 2010). An example of this is Netflix, a video-streaming service; the user provides personal information in order to gain access to the service. This is similar in definition to that of digital application. A digital application is a service that allows the user to "create, interact, collaborate and share in the process of creating as well as consuming content" (Obar & Wildman, 2015, p. 746). The term digital application came into use with the introduction of Web 2.0, an ideological and technological shift that enabled the digital user to not only consume content but also actively create it (Obar & Wildman, 2015). An example of a digital application is a social media platform such as

Facebook or Instagram; these sites allow users to create and engage with content via a digital venue.

Social media is another concept discussed at length in the following pages and is therefore important to define. Social media is a term used to describe forms of media that involve interactive participation (Manning, 2014). Social media serve as platforms in which digital users can create and publish content in a collaborative fashion, allowing individuals to be as involved in the process of creation of content as they are in the consumption of content. The term user-generated content is the activity by which a user creates digital content; this activity serves as the lifeblood of social media and fuels the maintenance of social networks online (Obar & Wildman, 2015). An example of user-generated content is the personal information a user enters in creating a virtual profile on a social media site such as Facebook, or liking a comment another user made on their social media profile, or commenting on a post about an event happening in your local town. These examples illustrate the kinds of content that fuel social media sites; engagement between users is necessary and without it the purpose of social media is defeated. Lastly, the terms digital technology and digital device will be briefly defined. A digital technology is one which generates, stores, and processes electronic data (Dunning, n.d.). A digital device is the mechanism by which users can access digital technology. Digital technology is found not only in computers but also in a variety of devices including cellphones, digital cameras, refrigerators, and e-books.

Finally, because the concepts of privacy and surveillance are discussed at length throughout this paper and serve as foundations to the conclusions made, I will address how these are separate, but also how they connect, particularly in consideration of the current surveillance culture we find ourselves in. Privacy is a difficult term to define, as it is broad and applicable across many disciplines. This has resulted in fragmented understandings of the term and its correlates (Dinev, Xu, Smith, J. H., & Hart, 2013). Alan Westin, a privacy scholar, defined general privacy as the withdrawal of a person from society through physical or psychological means, either in solitude, or anonymity and reserve (Westin, 1967). Another definition, privacy as 'the right to be left alone' is perhaps most well known and was put forth by Warren and Brandeis in 1890 (Dinev et al., 2013). The right to be left alone, or ability to be reserved, withdrawn or anonymous,

as referred to in the above definitions, is threatened by the pervasive nature of modern-day surveillance. Described in further detail later on in this paper is the concept of 'surveillance culture' (Lyon, 2017) in which citizens actively engage in the surveillance of themselves and others through use of digital technologies. One's ability to live a private life and eschew use of the internet and digital technologies has become increasingly difficult (Rule, 2007). Further, even if one avoids use of the internet and digital technology (e.g. mobile phone, tablet) the surveillance that occurs in public spaces through commercial and governmental recoding makes remaining anonymous virtually impossible. The surveillance practices that people engage in everyday (use of social networking sites, photography and video in public spaces, use of digital technologies that track and record personal behaviour) reduce privacy. Corporations and governments, then, collect and aggregate this data for various purposes. Further, the surveillance that occurs via public recording devices (e.g., traffic cameras, and corporate security systems) also reduces the ability of individuals to remain private. Surveillance and privacy are inextricably linked and the pervasive nature of current surveillance practices has and continues to challenge the right to privacy.

Chapter 2

2 Literature Review

2.1 Context

Life has become digitized. Ubiquitous use of the internet and digital technologies has permeated everyday life, seeping into the routine practices of individual and institutional bodies. For individuals, the development of digital devices has created small and convenient machines intended to be carried around at all times and in most places. Wearable devices attached to physical bodies monitor one's activities and movements scrupulously recording every step, breath, and sleepless night. Mass volumes of information made accessible by the internet and technology have caused individuals to experience "information overload" from the constant clamor of tweets, rings, dings, and notifications, all issuing attention away from the task at hand (Groes, 2017). Social media has expanded the spatial and emotional bounds around which relationships are created and maintained. Through the facilitation of social exchanges by social media, people are now able to stay in touch with past and present friends (Stutzman *et al*., 2012; Livingstone, 2008). The internet and digital technologies have become enmeshed in everyday experience blurring the demarcation of 'real identity' from 'virtual identity', leading some to suggest 'the death of privacy' or as Zygmunt Bauman suggests, 'the end of anonymity' (Bauman, 2011). In a Pew Research Center report, Homero Gil de Zuniga, director of the Digital Media Research Program at the University of Texas-Austin, said, “By 2025, many of the issues, behaviors, and information we consider to be private today will not be so. Information will be even more pervasive, even more liquid, and portable. The digital private sphere, as well as the digital public sphere, will most likely completely overlap” (Rainie & Anderson, 2014). The collapse of anonymity has resulted in part from the omnipresent nature of modern forms of surveillance. Technology has afforded surveillance regimes to become incessant, evoking a sense that one is always being watched. Individuals now find it difficult to escape the bounds of technology use and surveillance as both have become intimately incorporated into every facet of ordinary experience. Furthering this effect, the uptake in technology use by institutions has cemented the establishment of these devices into bureaucratic process and policy. The

use of technology now occurs in healthcare settings (Zonneveld *et al.*, 2019), educational environments (Windschitl & Sahl, 2002), within banking systems (Sajić, *et al.*, 2018), and by governmental agencies (Sivarajah *et al.*, 2015). Utilization of technological services by major institutions reinforces the presence of the digital into modern life, not only for individual people but also for communities as a whole.

Widespread incorporation of digital technologies into daily routines has also increased the capacity and scope of data collection and aggregation practices. Digitized data is collected through mundane activities including offline and online shopping, banking interactions, and digital search history enquiries (Lupton, 2015). Surveillance cameras monitor public spaces throughout the world, capturing video and audio interactions in real time. This content is stored and used by government authorities and commercial agencies for a variety of purposes (i.e., prevention of crime, evidence for criminal investigations, traffic control, promotion of safety in urban areas and so on) (Chayko, 2016). The data or 'user-generated content' that is willingly provided by internet users on social media platforms such as Facebook and Twitter is also recorded and aggregated; these data include,

> What is said, the profiles of the speaker and the audience, how others reacted to the content, how many 'likes', comments, views, time spent on a page or 'retweets' were generated, the time of day interaction occurred, the geographical location of users, the search terms used to find the content, and how content is shared across platforms and so on (Lupton, p. 3, 2015).

Social media and digital technology has transformed separation of the virtual and real, the private and public. The details of people's lives are put on display through the posts they and others publish on social media sites. Under this model, data gathered from private lives become commodities circulating on the global market, available to be bought and sold for state and corporate purposes (Van Dijck, 2013). Individuals engaged online are no longer digital users but products; their fancies, fetishes, fears, proclivities and preferences are used to satiate the appetite of ravenous databases storing users' data.

Technological advances and widespread use of digital services including social media have enabled governments and sub-contracted security apparatuses to acquire

information about citizens, building profiles around individuals' virtually visible behaviours for policing and surveillance purposes (Hintz, Dencik & Wahl-Jorgensen, 2019). The intensification of state surveillance following 9/11 resulted from a lop-sided narrative justifying far-reaching surveillance of citizens in the name of national security. This notion of national security being secured through consistent surveillance of citizens has resulted in normalization of invasive forms of monitoring, ultimately minimizing the issue of personal privacy and individual rights (Van Dijck, 2013). An example of this shift in surveillance can be seen in the USA-PATRIOT Act. The Act expanded the ability of security agencies to use traditional and modern forms of surveillance on everyday citizens without needing prior legislative approval through search warrants and court orders (Miller, 2011).

In 2013, Edward Snowden, a contractor who was employed by the National Security Agency (NSA), gained access to information about secret surveillance programs run by the NSA and British Government Communication Headquarters (GCHQ). Snowden leaked documents to leading media corporations, exposing widespread government monitoring of citizens' digital activities and behaviours. These documents revealed the scale of the surveillance activities engaged in by the American, British, Australian, and Canadian governments on their own citizens. Data being accessed consisted of: telephone records, text messages, emails, and physical locations tracked by mobile devices (Lupton, 2015). The Snowden documents also showed that the NSA had access to telephone company (Verizon) metadata and mined the customer databases of Apple, Facebook, Google, Microsoft, and Amazon, all large internet corporations frequently referred to as the "Big Five" (Lyon, 2017). Unsurprisingly, revelations such as these have caused internet and technology users to question the security of their online information and communications. Indeed, in a recent survey on the fears of Americans, researchers found that corporate and government surveillance of internet activity represented some of the top concerns (Karsten & West, 2016). In another study on the perceptions of security in a post-Snowden era, 80% of adults agreed that Americans should be concerned about the government's monitoring of phone calls and internet communications (Rainie & Madden, 2015). Results showed an almost universal lack of confidence in common communication channels —landline, cellphone, text messaging,

email, instant messaging, social media —indicating an absence of mediated communication through which people feel very secure sharing sensitive information. Accordingly, the Snowden revelations have also affected digital engagement, with 34% of adults reported having taken at least one step to hide or shield their information from the government.

Situating the climate of increasing distrust towards government within a digital context is critical, as technological means have enabled security-oriented states to monitor and track human behaviour at unprecedented levels. However the threat of surveillance is no longer something that is solely external. Indeed, it is something that people now willingly engage in.

2.2 Surveillance Culture

Drawing on Charles Taylor's (2004) work on "social imaginaries" to explore the aspects of surveillance in social relationships and normative routines, Lyon argues that modern life can be characterized by unprecedented involvement of active participants in everyday surveillance mentalities and practices. Surveillance is no longer an intrusive act on the part of governments or corporations. It is something that citizens comply with, engage in, instigate, and even desire. On this basis, surveillance has moved from being an institutional means of social control to an individually internalized practice that constitutes the repertoire of everyday experience.

Surveillance culture, as defined by Lyon, is distinguished from the concept of surveillance state in that surveillance today extends beyond the characteristically Orwellian nature ascribed to practices of government monitoring and intrusion (see Lyon, 2017). Mass surveillance of citizens still occurs, but the hard data used for these surveillance programs is often sourced from soft data willingly provided by people through engagement in everyday online activities. The concept of surveillance society is also inadequate in explaining the current climate of surveillance. Surveillance society was used to indicate how surveillance— by police departments, governments, workplaces— was affecting everyday routines. Though this concept indicates the broad practice of surveillance undertaken by various regimes, it still emphasizes the external and imposing nature of surveillance *from the outside*. Lyon (2017) argues that surveillance culture is

distinct from the above concepts in that it captures the intrinsic ways in which individuals actively participate in the surveillance of themselves and others through engagement with digital technologies. The explosion of digital applications and services that are built on a sharing model promote and even compel people to self-disclose varying levels of personal information that would conventionally have been considered very private. The imperative to share online results from what Brake (2014) calls an 'ideology of openness' whereby users of social media are expected to be transparent, honest, and open with regard to their personal information. This narrative of openness serves the interests of commercial organizations through promotion of increased self-disclosure and data sharing, which in turn benefits the companies with a stake in interpersonal-mediated communications (Brake, 2014).

The pressure to share extends beyond the realm of social media. Obtaining access to certain websites and digital applications requires personal information, forcing the user to engage in a trade-off, giving up some of their data to gain privileges (Wood, 2019; Rainie & Anderson, 2014). Further, the introduction of wearable devices has made the practice of voluntary data-sharing commonplace, leading to the establishment of the "quantified self" (Lyon, 2017). The capacity to self-monitor that is afforded by these devices has enabled those who seek self-knowledge the ability to digitize their behaviours. In an effort to "lead better lives" users provide vast amounts of information to wearable device corporations, beefing up the databases responsible for storing aggregated consumer profiles (Lupton, 2016).

Surveillance culture is dynamically negotiated through technologies that induce a collective need to share information online. In theorizing why people engage in self-surveillance, Lyons explains that the pervasive nature of surveillance in its inseparability from digital technology makes avoidance of all forms virtually impossible. In this world, the normalization of surveillance into the everyday has caused some individuals to become desensitized to the scale of data collection and aggregation practices occurring. Further, the lack of transparency from government and corporate entities regarding surveillance and data mining practices has resulted in citizens not knowing what is happening to their data online (Hoofnagle & Urban, 2014; Turow, 2013; Turow, Hennessy, and Draper, 2015). Limited understanding of the threats and challenges that

accompany digital engagement can reduce individuals' feelings of self-efficacy. Despite expressing concerns about digital surveillance, many people instead respond to this culture of surveillance with resignation. Dencik and Cable (2017) characterize this response as a form of *surveillance realism*. In the following section I will address this notion of surveillance realism further, providing a definition and connecting its relevance to the sociology of digital resignation.

2.3 Surveillance Realism

Surveillance realism is described as a condition in which people come to see surveillance as an inevitable aspect of modern social life; this inevitability can lead some to feel resignation, loss of control, ambivalence, and powerlessness. Dencik and Cable (2017) use the term 'realism' to indicate the attitude and practice of accepting the contemporary situation that is surveillance culture, thereby hampering the imagination of other realities. For those who are wary about the surveillant state of things, efforts of active and continued resistance can be difficult to manage and sustain. In such an environment, digital users who have unease regarding privacy and surveillance practices come to manage these concerns through a position of resignation. In this sense, though they have a preference for privacy, they also recognize the limits imposed by technology which undermine their ability to protect such privacy. This is not to say that citizens are virtual slaves dependent on the whims of internet corporations and global security agencies. However what is conveyed here is the understanding of 'social media as ideology' as Lovink (2019) puts it; expressed another way, social media and the forms of surveillance that result, have come to create a new ecology defined primarily by its banality. Surveillance surrounds us like air, acting as essential to the infrastructure that underpins social practice and interactions. Users can negotiate with interfaces, challenge controls, and learn about computations but the engaging and unceasing pull of social media, technology and self-surveillance slides people into networked flows. Surely people can refrain from digital and technological use, avoiding membership on social media platforms and the like, still when they do engage individuals experience a lack of sway in their ability to satisfactorily conform digital services to their security and privacy preferences. Surveillance realism is this realization indeed, that the response of

resignation in regards to mass data collection and surveillance allows one to accept limited agency despite a desire for control, while still remaining digitally connected.

The concept of "capitalist realism" advanced by Mark Fisher (2009) forms the basis for some of the ideas at the core of surveillance realism. In his work, Fisher discusses how capitalism has become kneaded into the very fabric of contemporary society. Through this incorporation, capitalism comes to produce culture through the regulation of work and education thereby constraining thought and action. In employing this framework Dencik and Cable (2017) argue that surveillance can be represented in the same way. Like capitalism, surveillance has become so entrenched in everyday experience that it comes to constitute the only form of apparent and possible reality. The normalization of surveillance is internalized by people, causing individuals to re-appropriate patterns of monitoring and tracking as part of their daily experience. The consequence of a 'culture of connectivity' (Van Dijck, 2013) in which people share their "music, videos, pictures, ideas and texts" (Van Dijick, 2013, p. 161) is the coalescence of data into an infinite stream of information which is then aggregated and used by technological conglomerates. The data generated by user's everyday digital interactions converge with metadata, and behavioural and profiling data resulting in "big data," a valuable resource for data analysts and marketers alike. Determining governance of these pools of data has become a political hot button in recent privacy debates with legal experts warning against the monopolizing power that technological giants hold over personal data (Van Dijck, 2013). The key to regulating technological services depends on knowledge of how these systems work. However the algorithms that dictate system processes are secretly kept in the hands of corporations, beyond the purview of regulators' control. Further, platform owners' calls for openness, transparency and frictionless sharing are slyly directed to users alone as connective media companies are reluctant to share information about their data-mining practices and commercial strategies (see Van Dijick, 2013). The combination of lack of transparency on behalf of government and corporate entities regarding surveillance processes, as well as the normalization of surveillance into the ecosystem underpinning social life, causes people to feel ambivalence, confusion, resignation and powerlessness with regard to the surveillance culture in which they are embedded. These feelings are symptomatic of surveillance

realism: the recognition that one is surrounded by elusive yet banal constraints of surveillance despite their autonomous desire for control and privacy.

The prospect of having reduced control online causes some digital users to negotiate surveillance through varying levels of self-regulation in an attempt to maintain some agency within the limited parameters set by digital services (Hintz, Dencik & Wahl-Jorgensen, 2019). Ferreira, Sayago, and Blat (2017) found that not feeling in control of one's data was a reason for why older Brazilian adults preferred not to engage online. Rather than letting the public nature of the internet discourage them, respondents developed strategies that allowed them to produce content in a controlled yet personally meaningful way. This indicates a form of self-regulation on behalf of individuals in an attempt to protect themselves from online threats while still remaining engaged digitally. Similarly, in her study exploring teenagers' practices on social networking sites, Livingstone (2008) found that the participants in her sample were concerned about their data online; privacy for them meant having control over who could access their information. In attempts at exercising control, young people were met with two problems: the lack of affordances provided by the site in use (e.g., limited ability to tailor and manage settings in ways preferable to them), and the issue of limited literacy of the interface design of social networking sites. Young people expressed frustration with regard to the reduced capacity they had in catering their information-sharing to groups due to the restricted options Facebook provided. Further, many respondents lacked basic knowledge of the options afford by the site, causing anxiety and nervousness in navigating these settings. The importance of remaining digitally involved superseded the limitations respondents faced on social media sites as young people acknowledged their need to disclose personal information in order to sustain intimacy with their peers.

The above studies touch on the limited ability users have in maintaining control online through their engagement with technological services and sites. This is because the strategies that digital users employ to combat perceived threats to the security of their personal information occurs within the confines of the site in use. These confines are articulated in end-user license agreements (EULAs) or terms of service (ToS). EULAs and ToS set out the constraints and obligations users are expected to abide by in using social media platforms. These agreements do not represent laws but rather, contractual

relationships that delineate appropriate behaviour and norms surrounding platform use, privacy and property claims. Most ToS also include clauses about the right of platform owners to sell user's metadata to third parties (Van Dijck, 2013). The trouble with these agreements is that users often accept the terms in question without understanding them or worse, they simply click "I agree" leaving the virtual document unread (Turow, 2003). Further complicating the issue is that governance of ToS and EULAs is primarily held in the hands of platform owners with modification of these agreements changing based on technology and consumer demands. These changes often occur without users' prior consent leading to controversial moves such as the one pulled by Facebook's CEO Mark Zuckerberg. In 2010 Facebook disclosed users' personal data to online advertising companies without their consent. In response to public outrage, Facebook offered a new policy allowing users to opt out of sharing their personal data to third parties however, the option to restrict sharing was disabled by default causing users to have to tediously navigate 170 different settings to simply tighten this sharing (Keys, 2018). The above example illuminates this notion of limited user agency within digital environments; users can opt in or out of use of technological services however in the instance where a user opts in and institutes privacy settings, the corporation offering the service can disregard these preferences, ultimately evading compliance with standards set by the user. This type of scenario gives rise to surveillance realism in that digital users feel they have no power to control the flow of their personal data aside from the asocial act of complete non-sharing, or of complete technological avoidance. This feeling of no alternatives, that to be socially relevant in this world you must be technologically engaged, perpetuates the normalization of technological engagement and therefore surveillance, into the crevices of everyday life.

In developing their theory of surveillance realism, Dencik and Cable (2017) interviewed British citizens and British-based political activists on their experiences of surveillance, the Snowden leaks, and online privacy. They found that participants had a general lack of knowledge regarding data collection and aggregation practices. Though individuals expressed worries about privacy and state surveillance these concerns did not translate to active resistance towards technological services and surveillance systems. Instead, individuals aired feelings of resignation, ambivalence and lack of understanding

in regards to the topics of mass surveillance and the Snowden leaks. In understanding that individual positions of dissent lack the clout needed to influence critical change of current surveillance realities, individuals resorted to self-regulating their behaviour online in order to guard their personal information.

Other studies have found similar responses to the current climate of surveillance, echoing the condition of resignation captured in surveillance realism. These studies will be addressed in the next section, where I will frame how the response of resignation and other related constructs such as privacy and security fatigue, privacy apathy and privacy cynicism, relate in unique ways as forms of privacy response to the current surveillance culture.

2.4 Responses to Surveillance Culture

In investigating the privacy paradox, namely the discrepancy between people's expressed desire for privacy and their seemingly contradictory self-disclosure behaviours online, various studies have offered frameworks for understanding the attitude-behaviour disconnect. In a report titled "The Tradeoff Fallacy" authors Turow, Hennessy, and Draper (2015) found that a majority of survey respondents (58%) felt resigned to the inevitabilities of consumer surveillance and data harvesting on behalf of marketers. Further, when asked about their knowledge of how marketers use personal information online, 40% of participants lacked basic knowledge to make informed cost-benefit choices. Respondents also overestimated the extent to which the government would protect them from discriminatory pricing (unique pricing based on individual consumer profiles).

Another study conducted by Hargittai and Marwick (2016) found similar attitudes among participants. Using focus groups, the authors found that the issue of 'networked privacy' caused individuals to feel that despite the protections they instituted online, privacy violations were inevitable. The notion of networked privacy (Marwick & boyd, 2014) suggests that privacy online is a networked, social and dynamic process. In networked settings that are impacted by technological and social elements, the ability of the individual to control his or her data online is compromised. Hargittai and Marwick found that study participants resorted to various strategies to gain control over their data

but ultimately acknowledged the lack of autonomy they had in connection to data mining, identity theft, changing privacy settings, and networked social situations. In acknowledging the difficulties stemming from networked privacy and inevitable privacy violations, users were cynical with regard to the idea of opting out entirely from digital engagement. They viewed opting out as an unrealistic solution to these problems and thus, disregarded it as a viable option. In conclusion, rather than finding support for the presence of paradoxical behaviour (the privacy paradox), the authors argue that the sense of resignation and apathy expressed by respondents represented a pragmatic response to the networked environment they encountered. The decision to disclose information was based on their idea that privacy violations were inevitable regardless of disclosure; this caused respondents to believe that their act of disclosure did not necessarily pose additional risks. From this understanding, disclosure does not indicate "people don't care about privacy" but rather, that people care about their privacy but feel they have little say or ability in controlling it.

The above studies suggest that resignation plays a primary role in influencing how users interact with the digital environment. Echoing this result, the next study found evidence of resignation through analysis of a different concept namely, security fatigue. Stanton *et al*. (2016) define security fatigue as an attitudinal threshold whereby security becomes too hard or burdensome to maintain. With the constant bombardment of messages warning of the dangers associated with online use, users can feel overwhelmed by the incessant need to be on alert and informed regarding the risks to their personal data online. Through semi-structured interviews, the authors found that this sense of fatigue commonly manifested in feelings of loss of control and resignation towards protection of personal data online. In citing the failures of institutions and large multinational corporations to maintain the security of databases, respondents expressed an attitude of fatalism in regards to the notion of data protection implying that the possibility of adequate protection is nigh impossible considering the sophistication of current hacking regimes. Further, security fatigue caused some respondents to become desensitized to making privacy-related decisions altogether, signifying a kind of indifference towards the idea of control and autonomy within the digital sphere.

In a 2018 study with internet users in South Korea, authors Choi, Park, and Jung examined the role of privacy fatigue in online behaviour. Similar to security fatigue, they defined privacy fatigue as a psychological state of tiredness that can manifest into strain characterized by exhaustion, cynicism, and reduced self-efficacy. To empirically evaluate the impact of privacy fatigue on online privacy behaviours the authors created a measure of privacy fatigue comprised of emotional exhaustion and cynicism. They found that individuals with higher levels of privacy fatigue tended to have higher levels of disengagement (the extent to which individuals give up control over their information), causing them to put less effort into making relevant privacy decisions. Interestingly, privacy fatigue had a greater impact on online behaviours than privacy concern indicating that as a measure, privacy fatigue is useful in explaining why individuals disclose personal information online despite their high levels of privacy concern. This provides evidence against the attitude-behaviour connection, a tenet of which the privacy paradox is based. Rather than attributing the act of disclosure to mean a lack of concern over privacy, this study shows that disclosure can be a symptom of being tired and disengaged from the persistent threats to one's privacy.

Relevant to this discussion is the concept of privacy cynicism. In research conducted with German internet users, Hoffman, Lutz, and Ranzini (2016), propose a new model of privacy response comprised of various psychological responses; these responses culminate into what they coin "privacy cynicism." The authors define this model of privacy response as "an attitude of uncertainty, powerlessness, and mistrust towards the handling of personal data by online services, rendering privacy protection behaviour subjectively futile" (Hoffman *et al*., 2016, p. 47). Applied to privacy online, cynicism represents a kind of cognitive coping that allows users to engage online, taking advantage of online services without necessarily trusting in commercial and technological providers to protect them. In acknowledging their lack of control over unavoidable and overwhelming external factors, digital users relinquish personal responsibility over their data thereby avoiding cognitive dissonance. Despite their desire for control, users form the conviction that effective privacy protection is useless and therefore out of their hands. Focus group participants cited feelings of uncertainty, powerlessness, mistrust and resignation when discussing online privacy and their experiences on the internet. Similar

to the above studies, the role of powerlessness or lack of control caused study participants to feel that they could not affect the movement and use of their digital data, leading to a sense of weakened efficacy. Feelings of resignation were also brought up with a number of participants stating that they believed privacy protection was futile. In seeing no viable alternative to using the internet, participants continued to utilize online services despite their reservations regarding the security of their digital data. Mistrust was also a common attitude among participants. Users were suspicious of agents shaping the online environment (e.g., technological and commercial service providers) and skeptical towards the motives of other users. Finally many participants reported feeling uncertain about the kinds of risks that could threaten their online privacy. This was due to an overall lack of understanding of the digital environment. Interestingly, the authors found that higher levels of risk awareness were accompanied by increased feelings of resignation. Increased knowledge of the risks associated with use of online services can cause users to become more disengaged from digital privacy protection. This supports findings from work done by Turow, Hennessy, and Draper (2015) in which users with increased knowledge of information collection were also more likely to be resigned to efforts at privacy protection.

In connecting the above studies to the concepts of surveillance culture and surveillance realism discussed in previous sections of this paper, feelings of resignation, loss of control, fatigue, mistrust, and uncertainty touched on earlier represent the condition of surveillance realism. This condition results from one's seemingly inescapable immersion into surveillance culture. Unavoidable engagement in surveillance culture causes individuals to feel powerless over control of their personal information. With digital technologies plugging into every aspect of modern life, eschewing the use of social media, the internet, and digital services has become an alien concept for many. This knowing, either conscious or not, of feeling forced to participate in surveillance culture causes the condition of surveillance realism that is, of feeling resignation with regards to the state of widespread and uncontrolled data collection and aggregation.

2.5 Implications for the Privacy Paradox

Before moving on it is important to address how the previous discussion relates to the concept of the privacy paradox. In the above sections various psychological responses are noted and examined in connection to the surveillance context that forms our modern experience. These psychological responses illustrate how digital users cope in nuanced ways with the all-encompassing nature of surveillance culture. The concept of digital resignation, which acts as a common thread coalescing together the concepts mentioned earlier—privacy apathy, privacy fatigue, security fatigue, privacy cynicism—positions the digital user as dissatisfied with practices of pervasive monitoring yet undermined in their individual ability to enforce control over the flow of their personal data. This perspective does not view individuals as passive subjects accepting the surveillant state of things. Further, this perspective does not view individuals as irrational, unwittingly serving up personal information on a platter for capitalist and state interests. Rather, subjects are understood to be rationally responding to the undesirable situation they find themselves in through resignation. Despite feeling that personal attempts to circumvent the bounds of surveillance are ultimately futile, individuals still negotiate within the confines imposed by technological systems through various techniques including but not limited to avoiding use of websites, instituting privacy settings, deleting cookies and so on. With that being said, each user experiments with the bounds of technological algorithms in ways preferable to them, and for some this technique is straight resignation. The response of resignation is sometimes viewed as a practice of complete surrendering, where all qualms are dropped by the wayside and all that remains is a forfeited skeleton, devoid of autonomy. From the outside, resigned digital users are assumed to be disinterested in the protection of their information due to their inaction in preventing collection of their personal information. From the privacy paradox perspective, privacy behaviours are viewed as connected to privacy attitudes. Following this rationale, the absence of protective behaviours indicates a lack of concern towards privacy-related issues, however as demonstrated in previous sections of this paper, though individuals resign themselves to employing a host of privacy protective behaviours, this does not constitute a lack of concern per say. To the contrary, it represents a conscious decision to

engage with the digital environment in a personally meaningful way, ultimately reducing feelings of dissonance.

The privacy paradox is this notion that there exists an apparent contradiction between the level of concern people express and their willingness to disclose information online. In one sense, while people express having concerns about digital privacy, they nevertheless continue to engage with online services that collect and aggregate their data. These users provide personal information (e.g., their name, date of birth, gender, postal code, and email, etc.) in order to gain access to a given service. At the center of the privacy paradox is the idea that individuals evaluate their decision to disclose information based on a calculated assessment of the potential costs and benefits they may experience. Based on this reasoning, the internet user is positioned as a rational actor who understands and is informed regarding the realities of the online environment, including the possible risks and consequences associated with use. The paradigm of the rational consumer is partly sourced from the work of privacy researcher Alan Westin (see Westin, 1967; Westin *et al*., 1992). Through surveys conducted between 1978 and 2004, Westin created three classifications of privacy in which people could be grouped: 'privacy fundamentalists' (those who are highly concerned about privacy), 'privacy pragmatists' (those who have midlevel privacy concern and distrust), and 'privacy unconcerned' (those who have low levels of concern and distrust) (Westin *et al*., 1992). Westin argued that most people could be defined as 'privacy pragmatists'. According to his theory, those in the pragmatist category are wary about the security of their personal information online but they make a rational decision regarding the conditions under which they are willing to disclose their information (Draper, 2017). Rather than viewing this group as ambivalent about their privacy online, the portrait of 'the pragmatist' is one of rationality; a user who logically calculates the costs and benefits associated with disclosure of information against other options available to them. There are faults in this logic however.

Hoofnagle and Urban (2014) argue that the assumption that internet and technology users are informed regarding the risks associated with the use of various digital services is problematic. In their study, they found that participants misunderstood both the practices that comprise data collection and their legal rights to privacy online. In testing the model of rationality attributed to pragmatists, the authors found that

participants who would have been deemed pragmatists by Westin's standards, routinely failed quizzes that tested their knowledge of data collection and digital privacy rights. The authors suggest that consumers often do not understand the exchange involved in providing their information. This lack of knowledge does not indicate a lack of care or concern towards privacy, rather it exemplifies a level of trust consumers have in the legal system based on the assumption that their information will be protected should anything nefarious happen. Supporting the above study on the issue of reduced knowledge, Turow (2003) also found that American adults were largely uninformed of data flow practices. They were unaware of how organizations collected data, connected data bits to other parties, and how and what types of information was stored. On this basis, Turow rejected Westin's characterization of consumers as 'pragmatic,' reasoning that a pragmatic decision cannot be made when the costs associated with the transaction are unknown to the parties involved.

In more recent work by Joseph Turow and colleagues Michael Hennessy and Nora Draper (2015) the authors challenge the subject at the heart of the privacy paradox in proposing that the act of disclosing personal information can be explained as a result of both lack of awareness of the consequences of giving data online and a lack of understanding about the mechanisms through which data is collected and used. Their research suggests that people have adopted an attitude of resignation towards protecting their personal data online because they believe they cannot change government or corporate policy, which if able, would allow them to have greater control to manage their data. Further, they feel if they disengage from use of technological and online services that they will suffer economic and social penalties. These factors taken together encourage adoption of an attitude of resignation; a sense that while a consumer desires control they feel they will ultimately never achieve it. This helps to get at the heart of surveillance realism. The lack of knowledge about digital infrastructure in conjunction with the omnipresent nature of digitally mediated society causes people to feel like there is no alternative to the surveillance culture, that there is no alternative to being watched and analyzed in everyday life. This leads to digital resignation.

The assumption that individuals are unconcerned about their privacy online because they refrain from employing privacy protection presents an incomplete picture of

what is going on. Digital users who do not protect their information online or who willingly provide sensitive details of their information online should not be assumed to be unconcerned; the position of resignation offers a new framework for understanding how despite pressing privacy concerns, individuals continue to engage digitally often sacrificing complete privacy as a result. The elusive nature of digital infrastructure in combination with the sheer ubiquity of surveillance through use of digital technologies causes people to feel resigned to the antiquated notion that privacy and anonymity can actually be achieved. The focus of this paper is on the sociology of digital resignation however this brief discussion of the privacy paradox was intended to poke at the logic connecting privacy attitudes and behaviours. Digital resignation offers a model that opens up the limited relationship of attitude to behaviour previously ascribed to digital users; such opening up is crucial for understanding the nuanced nature of digital privacy and how it is managed within surveillance culture.

Chapter 3

3 Methodology

The present paper uses 2013 interview data from the fourth study of Toronto's borough of East York (the Networked Individualism Study). The overall goal of the Networked Individualism (NI) study was to investigate the ways in which individuals were connected to their networks both online and offline. More specifically, the research examined how Canadians communicated with members of their social networks including friends, family, co-workers, and neighbours. Both open and closed ended questions allowed study participants to expand on topics personally meaningful to them, which proved useful for analysis regarding the complex, content-specific, and nuanced nature of privacy on the internet. The interview format explored:

- Forms of social support provided and received by participants' various networks (family, friends, neighbours, coworkers).

- Participants' privacy protective mechanisms: analysis of their use of passwords, aliases, computer protection software, and privacy settings on social networking sites (SNSs). Avoidance of certain websites and online services was also examined as a means of privacy protection.

- Participants' online disclosure practices: examination of how much personal data they disclosed, which types of personal data were disclosed, and which platforms were used to disclose personal information.

- Participants' concerns and attitudes about privacy: their self-reported privacy level, their concept of digital privacy and safety risks, and their view of others' privacy, e.g. family, especially children, friends, and coworkers.

- Participants' use of and opinion regarding various technologies including: mobile and computer devices, location-sharing applications, video calling and video conferencing applications, mobile finance and banking applications, instant messaging applications and SNSs.

- Participants’ opinion of the concept of reachability: whether they feel like they need to be reachable, whether location alters the way they communicate, and the medium of communication they prefer to use.

The interview structure started with questions regarding participants' demographics, level of technological understanding, and preferred methods of communication (both

online and face-to-face). In subsequent sections, participants were asked about their level of social connectivity and reachability, SNS use and behaviours, and experiences and attitudes regarding privacy and personal information compromises. For participants with children under the age of 18, an additional set of questions were asked to probe the types of concerns parents have with respect to their children's online practices and the potential risks, specific to younger age groups, that may be encountered. Although complete interview transcripts were examined and utilized for this study, this paper primarily deals with the privacy-related data. In total there were 88 questions as part of the interview format; some of these questions were directed only to individuals with dependents under the age of 18. The privacy-related data, of which this study is primarily based, began at question 73. This question asked whether or not the participant felt they were a private person. From this point, questions delving into feelings of privacy, management of privacy, and digital behaviours and their relation to privacy were examined. A benefit of the methodological approach employed in this study, was the depth of data provided by participants regarding their family situations, peer networks, work experiences, and cultural influences. This information provided a more in-depth understanding of the participant and how these variables impacted and connected to their feelings about privacy.

3.1 Data Collection

The sample was collected through a sampling frame of 2321 East York residents obtained from a Toronto-based sampling company, Research House-list services. Through random selection, 304 potential participants were recruited via letters to participate in the study, of which 101 agreed (a 33% response rate). Participants received an information letter outlining the purpose of the study, were invited to participate (which was approved by the University of Toronto's Research Ethics Board) and were offered a $50 coffee shop gift card as compensation for their involvement (see Quan-Haase et al., 2017 for procedural details). Participants interested in being involved were contacted via telephone to set up in-person interviews. After pilot testing, trained researchers and social science students conducted face-to-face interviews in English between 2013 and 2014. Interviews took place in various settings (e.g. in the interviewee's personal residence, coffee shops, and parks) depending on the preferences of the interviewee.

This paper is based on data sourced from in-depth, semi-structured interviews, ranging in length from 60 to 120 minutes. Due to the scope of content covered in the interviews, rich data resulted with roughly 35 pages of text for each study participant. All interviews were recorded with permission and transcribed by 14 assistants, with 59% randomly selected for accuracy by a third party not involved in data collection or transcription (Quan-Haase, Mo, & Wellman, 2017). Each study participant was given a pseudonym, reflective of their gender and ethnicity, to protect the confidentiality of the interviewees.

3.2 East York, Toronto

East York is a former borough of Toronto, Canada. In 1998 the municipalities of East York, York, North York, Etobicoke, and Scarborough, amalgamated into what is now considered the City of Toronto, the fourth largest metropolitan area in North America with a population of 2.9 million residents ("Toronto at a Glance," 2019). East York (2016 population = 109,468) is an upper-working class/lower-middle class suburb with housing styles ranging from detached and semi-detached homes to high-rise apartment buildings (Wellman, 1979; Quan-Haase et al., 2017). It is geographically bounded on the west by a highway and on the south by a subway line making travel of main routes accessible. It is located about six miles east of Toronto's business district, making it a half-hour subway ride or drive to the downtown area.

The area of East York has served as a hub for research through studies conducted by the NetLab at the University of Toronto. Beginning in 1968 and continuing through to the present day, numerous studies examining the nature of community and kinship, personal networks, and social support have been conducted (Wellman, 1978; Wellman & Wortley, 1990; Wellman et al., 2006; Wang, Zhang & Wellman, 2018). Over this period East York has undergone several changes documented by previous research. For the purposes of this paper, the process of referring to previous research conducted on East York has been valuable for understanding how the borough has changed across decades. Although the same population of people could not be studied, as multiple longitudinal studies were not feasible, East York retains importance for making comparisons between the pre-internet and internet eras (Mok, Wellman, & Carrasco, 2010). Further, the data

used in this paper are not new and has the benefit of being researched and compared across other studies (Quan-Haase, Mo, & Wellman, 2017; Quan-Haase & Elueze; 2018; Quan-Haase, Williams, Kicevski, Elueze, & Wellman, 2018; Elueze & Quan-Haase, 2018).

In initial studies conducted on the area beginning in 1978, inhabitants of East York were predominantly Canadian born or of British-Canadian descent (Plickert, Côté, & Wellman, 2007). The once homogeneous social backgrounds of residents shifted as their children and kin became dispersed throughout North America, causing a break to their insularity. Further, immigration and high-rise apartment development have transformed the once village-like integrated borough into a complex multicultural community, reflecting much of the surrounding metropolitan area (Mok *et al*., 2010). Individuals who were born outside of Canada represent almost half of this sample (40%), which has provided for ethnically diverse data to study. Moreover, due to the open-ended format of the interviews and nature of the questions being asked, interviewees were able to discuss their ethnic backgrounds and the relevance their ancestry has had to their social experiences allowing for incredibly nuanced responses (see appendix A).

Finally, as a result of immigration to Toronto and low mortgage rates, home prices have increased leading to populations being unable to afford buying property (Adela & Diana, 2018). According to the Canadian Real Estate Association (CREA) the average price for a Toronto home sold in 2011 was $465,369, with the average Canadian home selling at $352,600 (2011). Home prices in Toronto are higher than the national average as Toronto, along with Vancouver, represents a major market for real estate sales. With East York being conveniently located close to downtown Toronto, the economic value of this area has grown with expansion of financial and occupational opportunities based in Toronto partly fuelling this appeal. More than half (57%) of the sample resided in a detached or semi-detached home and the other majority (36%) lived in apartments. A small number of individuals lived in condos and only one individual was living in a housing cooperative (non-profit housing).

3.3 Demographics of the Sample

The overall sample is comprised of 101 participants, 57 women and 44 men ranging in age from 27 to 93 (the mean age is 58.65). Forty-one (40%) were born outside of Canada - in Asia, China, the Caribbean, the US, Europe, and Africa. Forty-nine (48%) were married and 24 (23%) were living with children under the age of eighteen. In terms of education, 3 (2%) had not finished the eighth grade, 18 (17%) possessed a secondary diploma, and 21 (20%) had completed graduate studies. Due to the age range of the sample, the employment status of participants varied. The majority of participants were employed (78%), eight (13%) were unemployed and 38 (37%) were retired. Participants were employed in various fields including medicine, law, education, information technology, and sales. This information was critical in gaining a comprehensive understanding of the contextual nature of participants' privacy attitudes and behaviours. For instance, many individuals worked in public sectors where they maintained visible profiles; these experiences impacted their views on privacy and how they tended to manage their personal information when using digital devices.

3.4 Internet Experiences

Respondents were asked about their self-perceived skill level in using digital technology and the internet. Options provided were: not applicable, not at all skilled, not very skilled, fairly skilled, very skilled, and expert. Most respondents fell into the following categories: fairly skilled (48%) and very skilled (23%), followed by one expert, eleven (10%) not at all skilled, eleven (20%) not very skilled, and 5 individuals who did not answer the question. Individuals in this sample saw themselves as relatively skilled and in supporting their evaluation they cited the ways in which they were knowledgeable online. These examples included but are not limited to, knowing how to send and download a file online, how to access and use the internet, use different internet browsers, use social networking sites such as Facebook and Twitter, connect various devices to the internet, utilize online applications such as online banking, and institute safety measures (e.g. deleting cookies, limiting access to secure sites, deleting suspicious emails and links).

All but eight (92%) respondents were internet users and of the eight, seven of them were aged 65 and older. Ninety-four (93%) respondents had personal access to a desktop computer or laptop; of the seven individuals who did not, 6 were in the 65 and above age group. To gauge the level of activity respondents had with regards to online services, they were asked about the kinds of sites they engaged with online. A majority of participants (59%) used Facebook, while 30 (29%) respondents refrained from use of any social media. To determine the relevance of privacy protection online, respondents were asked about the kinds of strategies they employed to protect their digital information and activity. Twenty-one (20%) respondents reported using aliases online, 74% reported having avoided a website because it required too much personal information, 83% of respondents withheld information on the internet or on social networking sites, and 54% of respondents had ignored or deleted 'friend' requests on their social networking accounts. As for device protection, only 33% of respondents reported utilizing software such as antivirus and firewall programs. Finally, 38% of respondents had limited or refrained from using their credit card online.

3.5 Data Analysis

The purpose of the Networked Individualism Study, of which the data used in this paper is sourced, was to analyze the ways in which individuals living in the East York area of Toronto were connected with their social networks. Qualitative research was suitable to meet the aims of this study because the nature of the topics considered (the role of privacy in online and offline contexts, the concept of social connectivity and its connection to technology, the frequency and types of technology used, and feelings regarding online and offline social networks) is complex. The open-ended, exploratory, and flexible nature of the qualitative method enabled participants to expand on their experiences, delving into issues personally meaningful to them. Questions that were pre-framed such as: 'Have you experienced privacy compromise before?' were probed further in an effort to more adequately understand the participant's feelings and ideas around issues. In acknowledging that knowledge is constructed through social, cultural, moral, ideological, and political contexts, we adopted a constructionist epistemological approach to analyze the data. From this stance, the notion that there exists an outside 'truth' to be discovered *out there* in the world is rejected. Instead, the construction of knowledge is

based on the discourses and systems of meaning that make up our reality, or our social situatedness (Braun & Clarke, 2013). In this way, the data is rich in that it allowed participants to reflect on their experiences in a thoughtful way, drawing on related ideas and their personal histories if they found them relevant.

Another important point to address regarding the qualitative framework employed in this study is the role of subjectivity and reflexivity. Subjectivity refers to the idea that our values, beliefs, experiences, preferences, and perspectives influence our understanding of things around us. This subjective position is intimately and inherently involved in the research process; rather than being seen as a bias to be eliminated, it is included in the analysis (Braun & Clarke, 2013). Reflexivity refers to the process of critical reflection regarding the knowledge that is produced and how this knowledge is then shaped by the researcher (Braun & Clarke, 2013). Being an internet user who frequently uses social media, online banking, and various applications, I understood in a personal way some of the experiences respondents spoke about. Though I have not experienced a breach or compromise to my privacy online, I am however familiar with some of the services and applications the respondents make mention of using. I am not devoid of internet and technological experiences where the responses of the study participants are completely foreign to me; rather I could understand some of their experiences on a deeper level having engaged with the same sites and applications.

In terms of categorization of the data, my analysis began with pre-coded and categorized information. The codes I initially referred to were codes covering the full scope of the interviews. The codes were created by trained academics utilizing the data for other studies (see Quan-Haase & Elueze; 2018; Quan-Haase, Williams, Kicevski, Elueze, & Wellman, 2018; Elueze & Quan-Haase, 2018). The initial set of codes mirrored the interview questions asked of participants. For example, one question asked participants whether they considered themselves private or not? (See Appendix A for reference). The corresponding code created was given the name: "considers themselves private" with participants responding "yes" coded as 1, "no" coded as 2, and "unsure" coded as 0. Each code was reviewed and edited if needed. Further, the support provided for each code was identified with a basic description, and note about the location (i.e., 75ci). Following completion of linking supporting quotes and interview content to the

initial set of codes, intercoder reliability was performed by an additional coder on 15 transcripts (15% of the data). During the collaborative process, codes that were not relevant were discarded as the aim of the study changed throughout the coding process. When differences in how information was coded resulted, a discussion regarding why decisions were made and the rationale behind the suitability of certain data to specific codes was addressed. Following establishment of codes we continued analysis until saturation was reached (when no new themes are found). The analytical process was strengthened through joint code development as it ensured that codes were clear, organized and thoroughly supported.

In analyzing the data, a thematic analysis was conducted. This qualitative analytic method is based on six phases of analysis, namely, (1) familiarization with data, (2) creation of initial codes, (3) identification of themes, (4) review of themes, (5) define and name themes, and (6) produce report (Braun & Clarke, 2006). Based on these phases an analytical process was created (see Figure 1). Data was categorized into five main overarching themes with one theme, mistrust, having five distinct subthemes. Excerpts used to support each theme were annotated with information about the participant (i.e., participant ID, gender, and age). In some of the selected excerpts unnecessary detail and irrelevant material was cut out; in excerpts where this occurred [...] was used to signal editing for this purpose. Finally, when salient features of the respondent were relevant, additional information was added to illuminate the excerpt. For example, one respondent discussed his experience being in the public light and how it impacts his concerns about digital privacy and his private life; in this case further information was provided regarding his occupation to give insight into his standpoint (see James McFinley, ID 24).

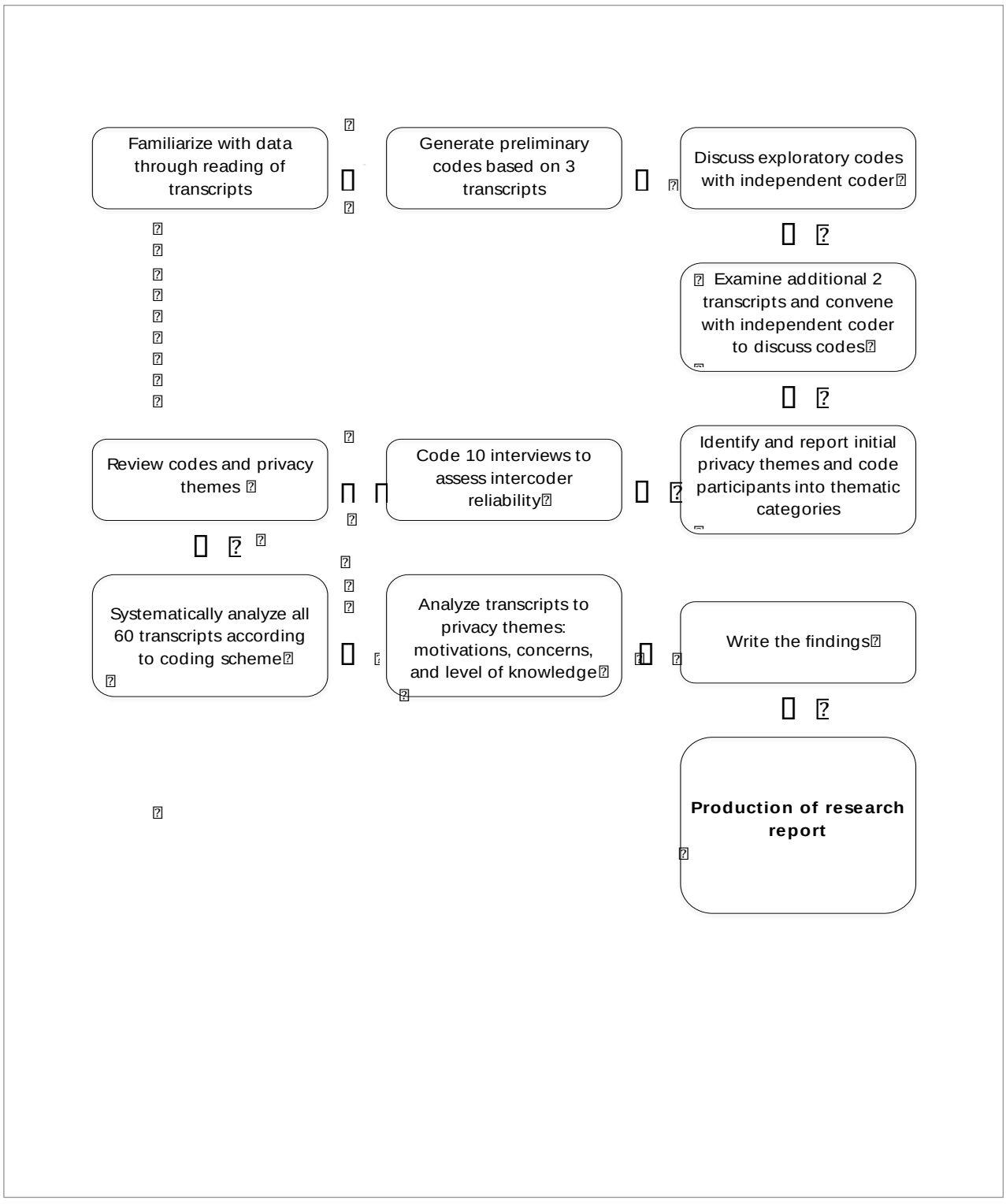

Figure 1: Thematic coding design employed for data analysis

Chapter 4

4 Findings

4.1 Mistrust

Mistrust emerged as one of the most prevalent themes in the interviews. The types of mistrust expressed by respondents included: 1) mistrust towards known others, 2) mistrust towards unknown others, 3) mistrust towards corporations, 4) mistrust towards government, and 5) mistrust towards technological and online services. Research has shown trust to be an important variable in influencing privacy related concerns and behaviours on the internet (Chang *et al*., 2013; Bansal, Zahedi & Gefen, 2016; Joinson *et al*., 2010). Applying the concept of cynicism to attitudes regarding privacy online, researchers found that user trust and correspondingly user mistrust, impacted the experience of many respondents in utilizing online services (Hoffman *et al.*, 2016). In acknowledgement of this, the presence of trust (or lack thereof) was examined while analyzing the responses of study participants in an effort to understand its impact on the privacy experiences of digital users. For the purposes of this paper, trust is defined as: "a psychological state that allows a person to accept vulnerability based upon positive expectations of the intentions or behaviour of others" (Chang *et al*., 2013, p. 440). Based on this definition, mistrust is the negation of the above, that is, a psychological state that disallows a person to accept vulnerability based upon negative expectations of the intentions of behaviours of others. In the following paragraphs respondents expressed mistrust towards the practice of online banking, interacting on social networking sites, using various technologies (e.g. iCloud, Skype), and conversing on public chat rooms.

Important to address here is that the final form of mistrust, mistrust towards technological and online services, overlapped with mistrust towards government and corporations. The creation and offering of online services is done through the efforts of an agent, whether that be a governmental body, an organization, or a corporation. When respondents express mistrust towards use of an online service, such as mobile banking or photo sharing and storage, they simultaneously yet inadvertently direct this mistrust towards the party offering the service. The decision to keep separate mistrust towards

technological and online services from mistrust towards corporations and government was because respondents would often make explicit and specific references towards a service rather than the provider of the service; this made maintaining the distinction between these types of mistrust important.

4.1.1 Mistrust towards Known Others

The first form of mistrust, *mistrust towards known others*, was a common issue for respondents. This type of mistrust was typically raised when discussing social media and the etiquette surrounding posting and discussing information online. Respondents reported experiencing mistrust towards people they knew either intimately or by acquaintance. Despite knowing these people, the respondents expressed doubt as to whether or not they could trust them entirely. An example of this type of mistrust was experienced by Meike Hallberg (ID 48, W, 53). In this case a direct incident led to the respondent feeling mistrustful towards her niece. She explained that her niece had become an atheist and the respondent sent her something online, intending for it to be private. Instead, her niece posted it to her public social media account creating conflict between the respondent and her brother (her niece's father). She discussed her feelings in the following quote:

> ...we talked, something about prayer cause she was, she's turned into an atheist and it's terrible for her, my brother and his, her mom. They're all very upset about it and I'm sort of in-between and I shared something with her and then she put it all over Facebook so, you know, my brother's wife calls me, “so I hear you don't pray anymore,” and I was like 'what?' This was private... So it's like yeah forget it. I'm not gonna connect with her anymore.

Although in the previous case the respondent's mistrust resulted from a specific experience, other respondents expressed feelings of mistrust towards people they knew despite not having a direct experience that led them to feeling mistrustful. Respondent Saad Bakkar (ID 41, M, 34) discussed being mistrustful towards contacts on his social media accounts because he believed people might use his connections against him:

> It's one of the drawbacks of social media and it's one of the negative tools that we have now. That people can make abuse of social media. People can see your friend circle. They can spread out any negative news for you, right? Even the LinkedIn also. People can see my connections and they can start campaign against me.

For these respondents, merely having contacts on one's social media accounts did not guarantee or predict any level of given trust. Indeed, others such as Howard Morton (ID 56, M, 60) discussed how he refrained from posting information relating to his sexual orientation online due to contacts he has on his social media accounts,

> ...my mother has a friend who – in her eighties – has a Facebook account. She has about fifty grandkids, I think, so that's why. Um, chances are I won't put something on there. I might not send her a picture of the pride parade. I could to anybody, anyway but yeah, I'll filter things down there.

The previous sentiments reflect a sense of unease towards the motives or judgments of others who are connected to their social media accounts. This may leave some respondents feeling on-edge or uncomfortable at the thought of what their contacts can access. It may also discourage individuals from feeling secure in what they choose to share on their social media accounts. This is connected to the concept of 'context collapse' where distinct audiences in one's social network are flattened out into a singular group of message and content recipients (Vitak, 2012). Respondents often discussed reservations about posting information on their social network account because their contacts represented a diverse audience leading to feelings of tension. With acquaintances, work, educational, and familial contacts converging in one's social network, separation of these groups can become difficult which can make posting of content and representation of identity more complex (Marwick & boyd, 2011). As in the above response, Howard Morton refrained from posting content connected to his sexual orientation because of a particular contact, his mother's friend, on his social network account. Audience and context impact the maintenance and forging of identity, both online and offline. The above respondent was uncomfortable posting about his authentic identity because of the

audience on his social network; this example illustrates the complex and problematic nature of self-presentation to diverse audiences online.

4.1.2 Mistrust towards Unknown Others

The feeling of mistrust was also directed toward *unknown others*, or put another way, people the respondents did not know personally. Due to the accessible nature of digital information and widespread use of online services, many respondents expressed concerns regarding the security of their personal information online. The internet has allowed unprecedented ability for people to be connected despite geographical distance and language barriers. This means people from across the world can now interact digitally, opening up a host of safety and security risks. Further, many online services do not have instituted systems intended to verify the accuracy of users' information. This permits opportunities for users to create fraudulent accounts not reflecting their authentic identity outside of the digital sphere (Lee, 2014). It also promotes a climate of deception, as there is no accountability for those that operate accounts using aliases and false information. The following quote by respondent Michael Harris (ID 4, M, 56) illustrates the uncertainty an individual can feel and the riskiness accompanying online communication involving unverified virtual identities,

> Yeah, because I think at least if you're speaking to a stranger on the street, you can tell whether or not they have any concealed motives. On a personal site like Facebook you can't glean any of that information, so you never know. And you don't know whether or not the picture that's on the Facebook site actually represents the person with whom you're talking, so.

Given the limitations with regards to verifying people's online identities, parents feel as though they need to be vigilant when it comes to potential risks to their children when using online services. Respondent Morgan Morris (ID 28, F, 53), a mother of a teenage girl, explained that her biggest concern for her daughter is predators,

> So I've seen a lot of shows like "Predators". People that you think you're talking to--like a good looking seventeen year old boy--turns out to be a sex offender or something like that. I watch a lot of shows like that which I find very interesting. I

> show my daughter, like "This could happen to you if you do this." Because you don't know who you're talking to on the internet. You just don't know.

Morgan illustrates a level of awareness regarding the risks of using online services. For parents, the threat of predators was a common concern. She went on to say,

> There are a lot of people out there who aren't well in the head so I tell my daughter all the time, "Do not ever give any personal information about yourself, or me, or where you live and no, never meet anyone off the internet, off of Facebook." You never know who you're meeting. A seventeen good-looking boy, when you meet him, is a fifty-year-old man. You know, I tell her, "Don't ever do that.

Many respondents discussed their efforts in guiding their children in how to detect predatory behaviour and refrain from providing any information that could compromise their identity. One mother, Gilda North (ID 35, F, 48) described how she teaches digital safety to her son saying,

> 'There are predators everywhere' you know and they could be everywhere you turn around, you don't really know anyone, that's the way things go.

The nature of online communication is such that the identity of people who use online services is in question until it can be verified. This is the case for those who use online dating services. Respondent Jason Smith (ID 66, M, 55) discussed his mistrust towards members of online dating sites and how people are untruthful in the information they provide,

> I find that the dating sites that I am frequenting…I find they're all on their playing games. You just like being my age and saying they're looking for something…again it's a lot about… I guess physicality and how someone looks and things like that…and how well they can make themselves come across on the thing…It's doesn't always pan out that way…A lot of game playing on there." Honesty…honesty…I don't want any…. I find there's so much dishonesty on there and BS flying around…I like to be honest.

Here, Jason acknowledges that some members using online dating services are dishonest with the information they provide. He mentioned how users of online dating sites represent themselves in misleading ways which has caused him to doubt the sincerity of the interactions that occur. For him, honesty is important when connecting with others on online dating platforms and he struggles with others being untruthful on these sites.

In communication with people met through digital venues, many respondents understood the need for ensuring their information was adequately safeguarded against possible breaches. Respondent Donald Yip (ID 52, M, 55), who has engaged in online forums and discussion boards talks about the safety precautions he would take to protect his personal information when communicating online,

> ... I joined a site where, about specific cars. I owned that type of car. Some guys would share information on, you know, what the problem with the car is, it has this kinda issues, if you want new brakes, buy these. This type of thing. It's all technical stuff about, about these specific cars. In that regard yeah, but I haven't, I haven't, you know, traded my email address or my personal address with these people or like, it's always just done on the site specific to that subject.

The respondent discussed how he never provides identifying material to people he met through forums. Further, he expected the discussion within these forums to relate directly to the purpose of the board, in this case cars. This implies a sense of etiquette regarding the function and expected communication of the online forum and indeed the respondent claimed he specifically used it to assist others in answering questions and to receive advice from other forum members about the subject of cars. In communicating with people online, Donald had clear set boundaries regarding the purpose of his interactions on the forum he used; discussions that went beyond the subject were not of interest to him. Similar to Donald, respondent Devon Edwards (ID 60, M, 70) who frequented online chat rooms explained his reservations with regards to providing his real name online,

> Well, I just, I was just concerned that somebody could…you know, like, ‘cause if I look my real name up online, I can find it. I’m there. I have, in the past, couple of

> times, I guess, I did reveal my name, and sure enough it comes up on Google. Google finds it. So I am there, if you look up my real name. But, but, of course most people don't know what it is, so they wouldn't know to look it up. But, uh, yeah, I don't know. I'm just worried that people might, um, like on a private chat like that, it's not so concerning. But on public chats where anybody can come on, I mean, you don't know who, you know, might take an interest and look you up, and they could find out where you live and so on. Because I'm on the phone book. You know. They could look you up on Bell and find out what your address is, and everything else. So. It's just when you're dealing with something as widespread as the internet, you know, that everybody has access to, that do you want to start revealing a lot of personal information? No. No, I don't think so. Just in case. There are some nutcases out there.

For Devon, the thought of his personal life being put at risk due to his involvement in online chat groups was a significant concern. He also discussed the distinction between private chats and public chats, citing the global reach public chat rooms can have. Ensuring his personal information was protected and not discoverable was important for the respondent especially in the context of public chat forums as virtually anyone can have access to these, increasing the risk for people in the absence of proper safeguards. Respondent Bethany Cobbler (ID 25, F, 40) echoed these concerns and expressed her doubts regarding the authenticity of people's identities online:

> I guess for the most part I don't really feel all that comfortable. The closest I've got to that is bulletin boards where people will post questions. I don't say "email me at whatever number". It's more question and answers about things like cruise shifts or writing a review. That kind of stuff. I guess I just don't know anything about them and you have to wonder if they're who they say they are or you wonder about safety risks.

This issue of mistrust towards unknown others was also a concern for individuals who had more public identities, mainly due to the nature of their occupations. As a known urban affairs reporter who writes about municipal issues, James McFinley (ID 24,

M, 32) discussed the need for him to keep separate his personal identity from his public and professional identity,

> ...I'm just anxious about putting that stuff online. I guess I'm a relatively private person, I mean I do engage in social media, I do use, obviously I use Twitter quite a lot but I prefer not to share anything that can be connected to me in the real world, if you know what I mean.

For this respondent, ensuring his personal information was protected was extremely important, as his employment in the political sphere had previously made him and his wife the recipients of hostile commentary online. Likewise, another respondent, Julie Lee (ID 99, F, 64) who depended on social media sites such as Facebook and LinkedIn to advertise for business, discussed her need in keeping her business separate from her personal life,

> The simple fact—and my home phone number—that it is my personal life and there has to be some delineation between business and home. So my clients don't get my home phone number. They don't, for the most part, know where I live. Because a) it's none of their business, and b) I don't want people knocking on my door.

Julie was purposeful about what information she provided in allowing her to be accessible enough for work while still maintaining boundaries for ensuring privacy in her personal life. Similarly Adam Ford (ID 46, M, 47), a principal, expressed his reservations about his public role and the visibility of his personal life,

> I like my privacy. I am very visible. I am a principal of a school with six hundred students. Although I don't live in that area, at work I need to be very visible. There's a huge accountability piece with my job so I am not a public speaker but I am very public. I do value and cherish my privacy, also the privacy of my children. Both my children are adopted. It is very important to me that when they are online they are safe and they have to be cautious about who contacts them. Maybe family members from previous lives, before we adopted them, we are scared of that.

Having adopted children and feeling the need to protect them from possible connections to their biological family contributed to the unease Adam felt with regard to his public status. The requirement of his job, namely that he be visible, inherently created increased risk for the respondent and his children. Individuals employed in fields that necessitate a public online presence, have to consistently manage the boundary between the public and the private in order to ensure their personal lives are protected.

4.1.3 Mistrust towards Corporations

In addition to the previous types of mistrust discussed, respondents also cited feeling *mistrustful towards corporations.* This type of mistrust involved questions regarding the motives of corporations, especially in connection to their online activities. Respondents were aware that regardless of the type, size or reputation of the corporation, the personal information of consumers could be used to benefit corporate interests. Respondent Carol Holman (ID 14, F, 36) mentions the advantages for corporations when people utilize their respective applications,

> I don’t know. I think a lot of those companies create those apps – cause, well, it benefits them – and then there’s people who do it, and I’m not sure why they think it benefits them. So I understand why those apps exist cause there’s always a, you know, corporate interest, but from the person’s perspective I don’t get why it’s fun to have the world know where you are. I don’t know, I don’t get it.

In the above quote, the respondent expresses awareness regarding the benefits corporations have when individuals opt to use their services. Moreover, this realization caused her to refrain from use of applications that had no personal value to her. Understanding that there exists a corporate motive behind the creation and offering of online services discourages some users from engaging in them. Indeed, Rebecca White (ID 21, F, 30) discussed her concerns relating to information collection on behalf of corporations and how she felt certain business practices infringe on basic human rights,

> I think I think with knowledge it's fine, I think the way that they go about it collecting information sneakily through third parties and stuff like that I think that's

> ridiculous. I think as consumers, as people we should have some sort of rights, some privacy rights that correspond with our human rights of privacy right?

She further went on to discuss Facebook and how users' information was provided to third party sources without providing individuals adequate information on how their information was being used,

> Right but then you're never really out of it because you sign up for something, you give your email here and it's like you have 300 people calling you where you don't know where they got your number from because they're selling it, third party information. Same with Facebook, they've just had issues with Facebook and privacy information because they weren't telling their existent people certain privacy rights that they didn't have, that they were being infringed upon.

Rebecca is referring to a case brought against Facebook in 2011. Facebook was charged with engaging in unjust and deceptive practices in violation of the Federal Trade Commission Act. The company had stated that it would keep users' personal information private then changed its privacy policy making the information public, without informing users of the changes (Bagley, 2019). In her statements, Rebecca alludes to a lack of corporate regard for the protection of consumer and users' personal information. She expressed her dissatisfaction regarding the absence of provisions ensuring the protection of users' personal information online.

Respondent Valarie Rosenfeld (ID 27, F, 40) also had concerns regarding the ability of corporations to keep consumers personal information secure. She cited a breach against Winners, a Canadian department chain, as an example of why she exercised caution in providing information to corporations,

> I'm more wary of corporations--I mean what happened with Winners, just a few years ago when they had that privacy breach with all those credit card numbers--I'm more wary of maybe retailers or organizations that might not have the same level of security as Canadian border security. So I think I would limit the information I would give out to a retailer, for example, for a loyalty program... I think it's my level--my perceived level--because there can be security breaches everywhere--it's

> my perceived level of privacy with certain organizations will dictate how much I'm willing to give out.

In her discussion, the respondent distinguished between the type of security used by Canadian Border Services to that which is used by corporations, such as Winners. She explains how the level of security offered by organizations and agencies influenced her willingness to provide personal information. In discussing the privacy breaches to Winners, Valarie expressed her reservations in giving information to retailers, inferring that she perceived the privacy protections they offer as being less secure than other agencies such as Canadian Border Services. Indeed, corporations that have previously experienced privacy breaches can discourage consumers from engaging and participating in programs and services they offer (Afroz et al., 2013). Moreover, in a public opinion survey of Canadians on privacy, results showed that most Canadians (85%) said that news reports on privacy breaches have impacted their willingness to share personal information ("2016 Survey of Canadians on Privacy," 2016). Similar to other respondents, Aaron Collins (ID 3, M, 69) described his reservations with giving information to corporations but mentioned how he reconciles concerns with the benefits he gains from using certain services:

> You know, for instance it’s just so easy to book hotels and things like that online. And you have some confidence that they're making their money by renting rooms, not by selling your VISA number to somebody, you know, if it's a chain or something like that. You have some confidence that it's not likely to be a problem. So you have a little concern that you really shouldn't be doing this but you do it anyway and it doesn't usually cause a problem.

The ways in which corporations financially sustain their online platforms and services are unknown to users and consumers. The above respondent acknowledged that there is a possibility that his information could be sold to third party sources but he continued to use the service, rationalizing his actions through a cost-benefit analysis.

4.1.4 Mistrust towards Government

A fourth form of mistrust, namely *mistrust towards government* was exhibited among many respondents. Concerns that were mentioned related to awareness of and worry regarding surveillance mechanisms used by governmental bodies. Respondents understood the risks associated with information being online and the possible uses it could have for government-related data collection and aggregation. Further, respondents also cited worries regarding data breaches and hacking towards government documents and collections of personal information online. The risk of identity theft was a common concern, with many respondents recognizing that even large corporations, government bodies, and financial institutions have the possibility of being hacked.

Respondents addressed the issue of government surveillance as being a concern and some made reference to Edward Snowden, a former American citizen who leaked government documents, exposing widespread and unauthorized surveillance of American citizens. Some of the respondents were interviewed in July of 2013, a month after the initial leak of governmental documents, making the case fresh in their minds (Fidler & Ganguly, 2015). Snowden and other whistleblowers (e.g. Thomas Drake and Chelsea Manning) who have used the Internet as an avenue to release information to the public, have helped to create a societal climate of suspicion and mistrust towards the concealed actions of governmental bodies. In understanding that a large proportion of the surveillance programs employed by governments are directed towards technological services (such as social media websites and digital applications) respondents expressed awareness of the fact that their information, personal conversations, digital search history and much more, could be surveyed by government sources. Respondent Brian Williams (ID 32, M 49) expressed his thoughts regarding Snowden and information collection on the Internet,

> Well I mean you know recently, that guy, what's his name? Snowden who revealed that the Americans were collecting all the internet facts. That makes you think about where things are... maybe there's no protection on the internet, I don't know.

In the above quote, the respondent expressed a lack of knowledge and understanding regarding data protection on the internet. He also mentioned how learning that information on the internet is collected prompts him to wonder about data aggregation and protection. Although news outlets promulgate stories about privacy breaches when they occur, the inner workings of technological services are not known to many people, leaving them uninformed as to the risks that accompany use of such services. Respondent Devon Edwards (ID 60) possessed a level of awareness regarding the risks of using online services though he attributed the issue of governmental monitoring to happening in the United States of America,

> It's been one of the items on the chat recently, has been all this NSA stuff in the States, you know, and the guy that's in Russia right now? Snowden? And, uh, the information he's releasing about all the information the US is gathering on people. Logging all their emails, their phone calls, their just about everything? God. That's terrible! There's no privacy down there at all anymore.

Though Devon's evaluation is correct and is based off of sources revealed through digital leaks of government documents, monitoring on behalf of governmental sources occurs globally, causing the internet to become a hub of data useful for governments around the world (Brake, 2014). In contrast, respondent Leslie Norman (ID 39, F, 62) expressed awareness in understanding that the government has access to her information online due to her use of digital services,

> I mean, I think that now on the computer they have access to everything anyways so really there is no privacy. Like, the bank has everything right? The government has everything. I mean you file income tax…online; your banking is online, like…I guess if you're smart enough you can figure it all out. Like you can get into all that stuff, hackers…

In engaging online and providing information through various means (e.g. use of online banking) Leslie recognized that this information may be accessed by various sources including the government. Connected to the above sentiment, an additional

concern many respondents cited in feeling mistrustful towards government was the issue of unsecure technological services. Some respondents were fine with voluntarily providing information to the government through digital means but their reservations centered on the risks of their information being hacked or accessed through privacy breaches.

Respondent An Dung Tran (ID 15, M, 71) avoided social media use altogether because he believed it was unsafe to have his information online and that systems could be hacked, even those used by the government;

> Not safe at all but now days even the government get hacked you a nobody, the more you are poor the less safe you are...

Similarly, Tom Michael (ID 55, M, 68) expressed concern over the privacy breaches towards government and financial institutions;

> I worry about the government and the privacy breaches we've heard about on CIBC. Their information of client's credit card information got out. They made good on all of it. Those are real ongoing issues that could possibly affect me.

Respondent Barney Rogers (ID 1, M, 44) discussed his view that the government should have secure systems protecting information, but even then, compromises still occur;

> I don't know, but I'm sure it's as safe as it can be, I would think, but then again the government, you figure they would have a lock on stuff and they end up losing stuff, so who can you trust? Nobody.

Utilizing online services that require personal and identifying information inherently places users in a vulnerable position as data that is stored has the potential to be compromised and used for nefarious purposes. Although online services institute mechanisms aimed at reducing the likelihood of breaches, the onus ultimately lies on the consumer, rather than the provider of the service, to ensure that they accept the terms and conditions, including the risks (Mitrakas, 2011).

4.1.5 Mistrust towards Technological Services

A final form of mistrust exhibited by many respondents was *mistrust towards technological services*. Common concerns that arose for respondents had to do with the aggregation of online data, the collection of digital search histories, directed advertising based on online activities, and the lack of control that accompanies use of online services, and the internet more generally. An important note regarding this type of mistrust is that it overlaps with mistrust towards government and corporations in that technological services are unilaterally offered through corporate or government entities. Apple Inc. is a corporation; however, it also offers a technological service (e.g. iCloud). When individuals express mistrust towards a technological service they also direct this mistrust towards the source providing the service. To illustrate this point, respondent Harry Jones (ID 42, M, 40) discusses a technology called iCloud. This service was created by Apple Inc. and it enables users to store and synchronize their data allowing them to seamlessly connect their wireless devices (Oestreicher, 2014). Harry questioned the security of the service and he expressed doubt regarding the protection of aggregated personal information. Moreover, his acknowledgment of his unawareness regarding the complex nature of the service, caused him to disengage from using it altogether:

> We don't have a Cloud because Cloud is a new concept...—I'm just one of those people who, the less I can keep my computer out there, the better. No one knows the vastness of how the Cloud works so how can we understand how to stop people from getting information. Any time you go online you're always at risk, one way or another. The minute you open up your browser. We try to keep everything pretty limited. We change our passwords every six months. We try to use very large passwords and do both combinations—characters and letters—jut to avoid anything. You have it happen once, and that's it. Even with Twitter and Facebook.

The concerns Harry Jones discussed are connected to his use of technological services and how to protect his personal information while using them. Although his mistrust towards the service also represented mistrust towards Apple Inc., it is more explicitly directed to a specific service that is offered rather than the company as a whole.

He also mentioned the ways in which he attempted to protect his information online, but recognized that through his use of online services he put himself at risk by engaging at all. Respondent Mark Voorhees (ID 10, M, 49) also expressed these feelings as he believed that anything put on social media sites can become public for all to see,

> My feeling is that if it's on Twitter or Facebook it belongs to the world. Don't try to be private on Facebook. It'll break your heart.

Although a user can enable privacy settings in an effort to reduce the visibility of their personal information online, risk nevertheless remains as the data can still become compromised and made public. This reflects an understanding of the ways in which technological services can be undermined through privacy breaches or changes to privacy policies. Connected to the above sentiments, respondent Shirley Ellsworth (ID 47, F, 48) explained how she avoided use of online banking systems because she understood the risks associated with use,

> That gets weird with me in terms of hacking or identity theft. So I wouldn't want all my documents to be in a digital place. I would not like that because of safety. It's a huge problem. I can't even imagine it not being a problem. In fact, because of that paranoia, I don't do online banking which is weird for someone of my knowledge and usage of the internet and I try not to use my Visa to pay for things online. I either get prepaid certificates or VISA cards and pay for it that way. I've known enough people that it just makes me terrible nervous about identity theft.

For Shirley, the possible compromises to her personal banking information make utilizing online banking services fruitless. Further, she purposely made use of safety mechanisms (using prepaid certificates and VISA cards) to reduce the probability of information compromise. In the same way as the previous examples, online banking services represent a financial corporation but rather than the above concerns being directed to the corporation, they are focused on the risks associated with use of an online service (e.g. online banking).

4.2 Perceived Self-Unimportance

Another theme that arose from the interviews was that of *self-perceived unimportance*. Respondents discussed their perceptions of their online activity and whether or not they believe it warranted attention from various sources including government and corporations. Further, a sense of resignation towards data collection and surveillance was predominant in some responses, indicating a level of acceptance regarding their digital and non-digital activity being tracked. Another unique aspect of this theme was that respondents commonly made comparisons towards their status as a digital user and the status of other digital users such as politicians and terrorists. They deemed politicians and terrorists as important users to monitor and attributed more significance to their surveillance thereby downplaying the relevance of their own online activities. However, other respondents recognized that their personal information was valuable and they had expectations relating to their data remaining anonymous. This attitude of perceived self-unimportance in relation to other users can be illuminated in the following quotes:

> Going back to the privacy thing. I usually think that there are so many people that are more interesting than I am, why would people bother, right? Whereas, you know, if you're doing exotic things on the internet then you'd become more interesting. I'm sure a politician would have to worry about every site he visited.

> Yeah, all kinds of people I wouldn't want accessing my banking information. But the Facebook stuff, by not putting anything up there that I don't want people to see. I'm not organizing bombing of the parliament buildings or something like that so you know, I don't really think CSIS is watching me or something, I'm not really too worried about it.

Here, Aaron Collins (ID 3, M, 69) mentions cases involving the actions of a politician and terrorist-related activities. He maintains that because his online activity is not as interesting or exotic as other users online, people are less inclined to monitor him. Further, he rationalizes his lack of worry about government surveillance of his online activity by inferring that his digital history does not necessitate attention from the government like others do. Aaron associates the aims of the Canadian Security

Intelligence Service (CSIS) a national intelligence agency, to the targeting of specific online activities (e.g. organizing bombings of government buildings). He explains that because he does not engage in such behaviour, he feels a lack of concern regarding this type of surveillance being directed at him. While it is true that due to limited resources and restrictions, the capability and reach of surveillance programs have to be set. However, recent advances in technology have allowed the surveillance net to expand, permitting the monitoring of people who are not necessarily targeted for surveillance (Rule, 2007). Similar to the above respondent, Carol Holman (ID 14, F, 36) maintains that she believes she is not important and that her online activity would not warrant attention from the government. She further goes on to explain that if her use of online services did receive surveillance then she would use software to prevent tracking of her digital activity.

> Um, as far as like the government watching what I do – if I were doing things that I felt were illegal or could get me into a lot of trouble, like even if I shouldn't be getting into trouble for them, then that might worry me. You know, if you're someone who does a lot of research on, like, terrorism then the government would want to start tracking you cause they think you're a terrorist. Is that fair? No, cause you're not a terrorist. You're just researching it. So if I were doing a lot of that kind of research then it might kind of bother me. I might start to use different software that would prevent anything I look at from being cookied or cached or whatever but I really don't think frankly I'm of any interest to any government or corporation except for as a statistic, if I'm one of a billion people who looked at something. So I just don't think I'm that important enough to have to hide myself.

In contrast, Mark Voorhees (ID 10, M, 49) discussed how his attitude of perceived unimportance is due to a combination of arrogance and low self-esteem. Unlike Carol Holman, Mark expressed how he believes he is 'bulletproof,' implying that he feels protected despite not instituting protective measures such as firewall protection or antivirus software. He explained how he assumes his virtual activity is not of interest to others,

> Well it's a combination of arrogance and low self-esteem. I'm arrogant enough to think I'm bulletproof and I have low self-esteem so I assume that nothing I have is of interest to anybody else.

Although the respondent acknowledges that his arrogance causes him to feel protected online, Mark also explains how his feelings of low self-esteem convince him that his digital data is uninteresting to other online users. The belief that one is uninteresting online may cause a user to refrain from instituting protective mechanisms in order to protect their data. For example, Aaron Collins (ID 3, M, 69) expressed his view that because he deemed himself uninteresting to others, he did not worry about security online,

> I don't think I'm of any particular interest to anybody. I don't have a hundred million dollars or, you know, there's a few private things... I guess I would try to protect that kind of thing, but I'm not really all that worried about Internet security.

In characterizing himself as uninteresting because of his financial status, the above respondent assumed his status as an online user was somehow less valuable, causing his level of concern regarding his online security to lower. This view is reflected in the work of Stanton, Theofanos, Prettyman, and Furman (2016). They examined how decision fatigue affected users' security decisions online. With the repeated surge of messages towards online users reminding them of the risks online regarding privacy breaches, identity theft, hackers, and lurking eyes, individuals feel inundated with the risks posed to them. Among the findings of the study was a sense among participants that their data was not at risk because they lack importance for others to care about their information. This attitude reflects the feelings of perceived self-unimportance indicated by respondents in this study. Similarly, in a survey probing Americans' ideas about domestic and international surveillance, a common response among participants was the notion that individuals perceived themselves to be unimportant; because they had nothing to hide, they did not feel threatened by surveillance programs (Madden, 2015).

Further research is needed to understand the prevalence of this perspective and consequences that can result as minimization of personal risk and devaluing of

information can be critical in impacting one's security online. The assumption that a user is not at risk because their online activity does not represent risky or interesting behaviour is a problematic position to assume. With surveillance programs expanding and information collection and aggregation processes becoming more sophisticated, ensuring that the online data of users is protected, kept anonymous, and cautiously and intentionally provided is important.

4.3 Loss of Control

When discussing their experiences online, loss of control was a predominant and recurring theme for respondents. Many users described feeling powerless over how their data was used and whether or not it would be protected. Facing forces that they perceived to be beyond their control, users felt as though they did not understand the mysterious workings behind the online services they engaged in. Based on this perspective, many respondents expressed a level of acceptance regarding loss of control once they shared their information online. They understood that by posting information on the internet, there was a chance that it could become compromised so acceptance of this fact was necessary in opting to share content. In discussing social networking sites, numerous respondents acknowledged the public nature of these sites and recognized the possible consequences of sharing information through these outlets. The mechanisms available to users using social networking sites make it difficult for individuals to control how their information flows between their contacts. Moreover, the constant changes to privacy controls and corporate policies act as an additional barrier for users in staying informed of relevant information regarding their privacy and how their personal information is used. David Brake (2014) argues that digital services are built on a content-sharing model and as such, they depend on users to self-disclose information. These services offer tools to encourage and nudge users to share and discourage the use of privacy controls. For users to properly utilize privacy tools they have to be informed of their capabilities and understand how to adequately manage their information; these conditions are difficult to meet when technical capabilities and policies rapidly change.

In examining privacy through focus groups with young adults, Hargittai and Marwick (2016) found that focus group participants expressed feeling little control over

their personal information online. Participants also cited feeling a lack of control over their information on the social media site Facebook due to routine changes to the privacy policies. Similar to the concerns raised by focus group participants, numerous respondents in this study described social media sites as a space where control is weakened, sometimes ceasing to exist at all. Respondent Mark Voorhees (ID 10, M, 49) explained,

> My feeling is that if it's on Twitter or Facebook it belongs to the world. Don't try to be private on Facebook. It'll break your heart.

Adam Ford (ID 46, M, 47) concurred:

> Well people that I like or I trust or I want to share it. On Facebook people can steal photos quite easily. Once it's on Facebook, it's out there. I know you can use adult privacy settings but once you're there, it's fair game. We try to educate our sons about what they have on there. Their digital footprints.

This idea that once data is online, it is open to compromise was a common attitude among participants. Respondents recognized their personal responsibility over their information online. For example, Donald Yip (ID 52, M, 55) expressed how he protects himself online but also recognizes that ultimately once content is posted online, it is open to abuse by others:

> These days you just have to be careful about who you contact and what you do on this computer and how you use this technology cause I don't, I just assume none of it's private I mean, and it, it really isn't, none of it is private. If it's digital it can be compromised in some way, in some way (34a).

The above responses illuminate the understanding some participants possessed concerning the lack of security of online information. Adam Ford recognized that his desire to share content with some people on his social media opened up such material to possible compromise should a breach happen. As well, Mark Vorhees expressed his belief that content on social media sites like Facebook and Twitter, belong to the world so attempts to be private are fruitless. An acceptance of lack of control is indicated by these

respondents as they expressed awareness that the internet, as with any media technology, is governed by various agents who possess power and influence in shaping the services they engage with and how their information is used, should they provide it.

The digital environment can act as a vacuum, sucking available information into a data hub intended for aggregation and analysis. Further, most internet services use cookies and subscription services to collect demographic and behavioural data about users who engage with their sites (Lupton, 2015; Brake, 2014). Respondent Tom Michael (ID 55, M, 68) explained his feelings on behaviour tracking online, saying:

> If I know why they're collecting it, I don't mind so much. But honestly, there are so many ways of collecting information... There are anonymous ways to get information without identifying yourself. It's an opportunity to target people through their emails and mail. You can start to lose control of who you really are with all the things coming at us. You don't know who is checking in on your database. People's behaviours can be tracked (74).

Tom acknowledged a lack of control regarding the actions of other users. He understood the different ways data can be collected (e.g. mail and email) and he expressed awareness that his information may be targeted and tracked. Several respondents expressed feelings of uncertainty regarding where their information would end up. When discussing what happens to her personal information online Veronika Valdas (ID 62, F, 73) said,

> Well it just makes me feel uncomfortable to have it go off into cyberspace and I not know where the hell it is.

Another respondent, Jason Smith (ID 66, M, 55) expressed his views on the unknowns of where his information goes,

> Oh just the same thing that I was speaking about you know the privacy and putting your stuff out there and…not being able to retrieve it or know where it is all the time. You just never know.

The nature of how digital information is stored, how it is categorized and organized, and how it is made anonymous are all processes relevant to users and use of their personal information; however, the intricacies that compose data collection and aggregation practices are unknown. Respondents expressed feelings of discomfort regarding the security of their digital information as they acknowledged that they lacked awareness of the processes involved in the movement of their online data. Further, due to lack of control and feeling insecure about the location of their personal information, respondents recognized the risks associated with having information placed in the wrong hands. Respondent Sean Fells (ID 36, M, 64) expressed his concerns for his son in posting information online and the possible risks to his reputation depending on the content shared,

> I'm always encouraging him to be discreet when he put things up because my concern is that once it's out there, there's no getting it back and we do know that employers and others do use, you know, like they check Facebook as a, when they're searching for prospective employees. I mean I think that would be less of a concern for a sixteen year old but if you're posting pictures at age twenty-two, depending on what those pictures are, could cause you problems.

In understanding that employers refer to social media sites such as Facebook to evaluate potential job prospects, the respondent preferred that his son be discreet online in order to protect his reputation. He goes on to say:

> Yeah... it's principally cause I just, I mean again it's, once you put it up it's, it's there and it's hard to get it down if, if at all and it again, like anything else in the world, it can be misconstrued.

Sean acknowledged the difficulty that can arise in trying to have content removed off of the Internet, inferring a loss of control over data once it is posted online. Digital information can become available and accessible to all users of the internet which in effect, opens up one's data to potential abuse by others. How information is taken and altered is beyond a user's control and can cause damage to one's reputation both inside and outside the virtual sphere. In a survey on Americans' attitudes of privacy and security, 88% of American adults agreed with the statement that it would be very difficult

to remove inaccurate information about them online (Madden, 2014). They felt that once information was online, their ability to control it, namely how it was received and portrayed, was weakened or erased completely. Extending beyond Americans, this attitude was also identified in an ethnographic study of Canadian internet users; respondents expressed their feeling that once content is posted online the user looses control over it and that any expectation that it be used in their interest is faulty (Viseu, Clement & Aspinall, 2004).

Similar to the above sentiment, Brian Williams (ID 32, M, 49) expressed awareness of the risks to information once it is released online:

> Just because there's potential for it to end up in the wrong hands, you know? Like Twitter, saying something stupid and then regretting it but then it's too late. Everybody else knows, it's not just a few people, it's the whole world can know.

The public nature of the internet and online services allow for vast connections to be made between parties across geographic and cultural lines. In saying the whole world can access one's information, the respondent's inference is not misguided; once a user opts to release information online, the opening up of compromise to that information occurs. Feelings of loss of control arise when one realizes that as long as their information is posted online it can be violated, despite security mechanisms. The creation and management of one's online presence, including posting of content, is serious when considered through this lens, as any material posted has the possibility of being accessed and used for either good or bad.

4.4 Agency

Despite many respondents expressing feeling a loss of control concerning their data online, being agentic and instituting privacy-protective behaviours remained to be an important measure in engaging online for respondents. Many discussed the obstacles they faced in gaining control of their data and how they felt about their data being used. There is evidence that American adults are concerned about having control over their personal information online. A 2015 Pew Research Center study found that 93 percent of adults reported that being in control of who got information about them was "important" and 90

percent said controlling what information was collected about them was "important" (Madden & Raine, 2015). Indeed, respondents in this sample expressed similar views and employed various strategies to protect their information and minimize risks. These strategies included using pseudonyms, enabling privacy settings, using software protection, refraining from use of certain sites and online services, deleting cookies, and limiting information they provide to online services.

Respondents frequently discussed the social networking site Facebook and their issues with the platform. Thomas Bailey (ID 13, M, 55) explained why he opts not to use Facebook,

> I'm not on Facebook. I've got some security issues with it. I don't really feel that a daily description of what's going on in my life is important to anybody else. Businesses that I work for have their own Facebook sites so I don't need...I can work through those I don't need to work through my own. And I guess maybe just...I'm a bit of a private person. I just don't share a bunch of stuff with a lot of people.

The respondent reasoned that due to his preference to be private, he refrained from using Facebook through a personal account. He also addressed his reservations about the security of the site and how this contributed to his disinterest in engaging on it. Due to a misalignment of the respondent's preferences and the services offered by Facebook, he opted out from membership on the site, demonstrating his agency as a digital user and consumer. Further, Thomas recognized that if he needed he could use Facebook through work accounts rather than through a personal account. In this way he adopted a strategy aimed at protecting his personal information through avoidance of membership, while still gaining benefits through utilizing the site through different business accounts.

A concern mentioned by respondents in discussing their lack of control in using online services was the repeated changes these services would make to their privacy policies. Respondent James McFinley (ID 24, M, 32) also made mention of this issue but addressed it through discussion of his agency. He expressed how he made consistent

efforts to ensure he remained informed regarding the changes to Facebook's privacy policies.

> Well as much as possible I rely on Facebook's privacy settings and I try to make sure I'm understanding that any time that they make a new change or whatever to their privacy policy.
>
> I guess it's just more than anything it's just a sense of wanting to maintain that control not that I have a wildly exciting life that I think people are necessarily even that interested in but I would prefer to be in control than not.

Although he recognized the lack of control that he had over the repeated changes Facebook made to their privacy policy, James nevertheless exerted agency through his effort to maintain knowledge of these changes. Rather than resigning himself to the changes being made he instead adapted his behaviour to respond to the digital environment he encountered. In discussing social networking sites Harriet Morris (ID 23, F, 52) explained that she was cautious when using social media because she found the line between sharing while not sharing too much information difficult to manage:

> So for me I've really found the transition to social media difficult and I still find it difficult because I don't want to put all this stuff out there. I will share things that I want to share but it's not that often. Most of the time, I'm also very cautious.... I just like to draw the line between too much information. So naturally being a very private person but also being Gen X and growing up with a certain level of privacy. A lot of Gen Xer's that I know---with that whole Big Brother thing--are worried that with too much personal data out there, Big Brother's watching over you. So you tend to be a lot more wary about what you're putting online, because it's out there forever. It can really be pieced into a profile of yourself.

In the above response, Harriet recognized her lack of control about surveillance (in mentioning Big Brother is watching) yet she continued to exercise control in that she mindfully and carefully chose the content she would post on the site. She also discussed how the transition to using social media was difficult because the expectation of sharing and being open did not align with her personal need for privacy. In responding to her

needs, she purposefully utilized the service in a way that enabled her to be comfortable and feel in control of the content she did decide to post.

Similar to Harriet Morris, Catherine O'Henly (ID 53, F, 67) understood that her personal data may be used for various purposes but in contrast, she wanted to remain anonymous, having her personal identity kept separate. She was willing to provide her information given that she could have control of her anonymity,

> You're not going to use it with my name attached to, to anything so it doesn't really matter, I'm just a nobody in your collecting the information.

Similarly, Sean Fells (ID 36, M, 64) expressed a need to remain anonymous in aggregated information in order to protect his identity,

> I don't have a problem with organizations collecting information if it's aggregated but if it's used for specific purposes directed towards me then I have a real problem with it.

For the above respondents, their willingness to provide personal information for various uses was based on the assumption that it will remain protected and anonymous. As agentic users, use of their personal information was acceptable according to the above conditions namely, that it remain protected and anonymous; if these conditions cease then use of their information would no longer be acceptable. Reservations articulated by the above respondents reflect the attitudes of other Canadians as 90% of individuals polled in another study expressed at least some level of concern regarding use of personal information by companies or organizations ("2016 Survey of Canadians on Privacy," 2016). In understanding the risks associated with information being used by corporations and organizations, the above responses illustrate a level of awareness regarding the risks associated with connection of virtual data to personal identifying data. In contrast to the above respondents, Thomas Bailey (ID 13, 55, M) refused to share his personal information because he disliked not being informed as to what was happening with his data and where it was being directed:

> I don't share it because it irritates me that they're collecting data without giving me some sort of reasons to what they're doing with it or why they need it. Same thing, telemarketers just drive me absolutely crazy so yes, I've got my number blocked for whatever good it does. But that...I consider that an invasion of my privacy. If I want to buy something I'll find it and I'll buy it. I don't need somebody coming to me offering to sell it to me (74a).

The lack of control felt with respect to how Thomas' personal data was used caused him to refrain from providing his information altogether. In asserting control over where his information was going and what he allowed to be accessible, he avoided providing any data to ensure his privacy was not being intruded upon. This theme of agency is important as it illustrates the efforts individuals make to protect themselves online and reconcile their needs with the uses and restrictions offered by online services. Despite many individuals experiencing cynicism, exhaustion, apathy and resignation regarding the relationship between the digital environment and their personal information, others continue to make efforts to protect their data, remain informed, and act autonomously in their digital interactions.

4.5 Resignation

Due to the lack of control and feelings of powerlessness that can result from use of online services, many users feel resigned towards risks to their information online. Scholars have studied how resignation impacts the attitudes and actions of digital users. Through interviews with American adults, Stanton, Theofanos, Spickard-Prettyman, and Furman (2016) found that feelings of security fatigue, when security becomes too hard or burdensome to maintain, often manifested as feelings of loss of control and resignation. The authors found that participants adopted a sense of fatalism regarding control of their information online in that they viewed their efforts to protect themselves as futile due to evolving technology, changing policies, and the persistent risk of breaches. Similar to the concept of security fatigue, authors Choi, Park, and Jung (2017) found that in their study examining the online experiences of 324 Internet users, privacy fatigue was shown to have a strong impact on privacy behaviours online. They define privacy fatigue as a "sense of weariness towards privacy issues" (Choi, Park & Jung, 2017, p. 42). This

response towards online privacy can cause individuals to put less effort into making privacy decisions, withdrawing and disengaging from management of their personal information due to feeling a loss of control.

Respondents in this sample indicated feeling resigned to privacy risks online and similar to the above studies, respondents also felt that any effort aimed at protection of information was ultimately futile. The combination of feeling a loss of control, feeling uninformed as to what was happening with their data, and believing there were no alternatives available to them, respondents suspended their need for control and accepted the associated risks of engaging online. Respondent Andor Mills (ID 71, 64, M) expresses his belief about information control online:

> Everybody's got our information. There's a lot of information on us out there but there's nothing you can do about it anyway.

When discussing the topic of data collection and governmental surveillance, Devon Edwards (ID 60, M, 70) expressed his belief that widespread practices of monitoring were not beneficial. When probed to see if he had taken any steps to prevent his data from being collected he responded by claiming that any efforts aimed at preventing intrusions of privacy were futile because they would gain access regardless,

> Well, no. I don't think you could in that case. I mean, if they're going to monitor your emails, they're going to monitor your emails.

In the above responses, there is a sense of giving up of full control and an acceptance of a lack of security. Rather than indicating ways of coping with a lack of control online and citing examples of strategies they utilize to combat compromises to their privacy, they instead maintain a passive approach towards their online data and use of online services. They accept the possibility of data breaches and resign themselves to a position void of control because they believe they cannot affect the potentiality of threats to their data. When asked about how other people navigate privacy concerns online, respondent James McFinley (ID 24, M, 32) said:

> I think they've all sort of made their peace with the fact that you know Facebook knows everything about you.

The above concern is not unwarranted. A dark side of the internet is the problem of data collection and aggregation. Every interaction a user has with the internet, social networking sites included, is archived and made accessible. The promise of forgetting no longer exists in a digitally mediated society, as routine aspects of everyday life are recorded and stored indefinitely (Simanowski, 2018). Once information is released online, the user assumes personal responsibility of compromises that may occur. This feeling of responsibility wanes when users feel like they lack power over control and management of their data. Respondent Aaron Collins (ID 3, M, 69) discussed his view that privacy is non-existent and although attempts can be made to protect one's data, ultimately the guarantee of privacy no longer remains:

> I'm not concerned about you know, somebody has my social insurance number or VISA number because I think people are kidding themselves when they think that they have privacy... you know it's a big thing now, you shouldn't let anybody know your social insurance number. When I first started doing income tax back in the sixties, you used to get your income tax form with the social insurance number printed right on the cover, right? Nobody cared... I mean I don't really believe that there is that much security for things like bank accounts, you certainly try to use passwords but... I mean there's things that you can do but I think you're kidding yourself if you think you can be private.

Aaron also goes on to say that he accepts his lack of privacy because he understands that technology has faults and breaches can still occur:

> So we have Norton on the computers and it certainly seems to cut out bad stuff but it won't surprise me if some virus gets through because, you know, nothings perfect. So I'm fairly okay with lack of privacy.

Echoing Aaron's sentiments, Sidney Cooper (ID 26, F, 68) feels that despite her efforts to employ use of a password to protect her activity online people could likely override this, gaining access to her accounts:

> I guess that's the only way of protecting it. I try to use a password that isn't…wouldn't be easy to spot you know? Or easy too log into but I could probably be fooling myself. I'm sure…I'm sure anybody can get into something I've got as a password.

Harry Jones (ID 42, M, 40) feels a similar way about the limited security he encounters online,

> I feel my safety is at risk every time I log on but, you know, to a varying degree I know that it is relatively safe. I do whatever I can but generally speaking I think there's a relative safety but the minute you go online…there's a possibility.

The commonality in the above responses is this idea that regardless of the security measures put in place in order to protect one's information online, privacy is no longer a guaranteed right and breaches can happen despite these implemented safeguards. This view, that if one is going to engage online they assume the risks that are associated with digital engagement was also indicated in Donald Yip's response regarding use of digital technology. In this response he also discussed the feeling of having no alternative to life with technology, that if one is interested in engaging online, or if a person wants to interact with the world around them, use of technology is unavoidable. He mentioned his idea of an alternative to no digital interaction being living separate from people and technology altogether:

> Obviously the bank knows where the hell I am. They have my address, I mean you know, let's get, let's be realistic about it, you know, like since time's started people have known where other people lived. You know like you can't, unless you wanna live up in Northern Ontario in a shack and be, and completely opt out of all kind of technology, that's the only way you're gonna stay away from anybody, right? Soon as you have a cell phone, you know, they'll find you through triangulation so they'll, they'll find you. So I'm not too worried about it, you just have to, I mean I'm not paranoid, I'm not a conspiracy theorist so I'm not too, not too worried about that but I'm just very careful about who I give my information to and that's, that's the way you have to be these days, as far as I'm concerned.

> You know, it hasn't, it hasn't, I haven't been compromised yet. I'm sure I will but cause it's really tough to safeguard yourself...

At the end of his response, a sense of resignation is illustrated; Donald maintained that although privacy compromise has not occurred towards his data and that he attempted to protect his information online, the possibility and even inevitability of compromise would occur. In this way, online users may ardently endeavour to protect their information online while also understanding that the safeguards they've instituted may not be enough, and may lead to a breach of their security. In discussing his reservations regarding what others post about him on social media, Barney Rogers (ID 1, M, 44) expressed his experience of not being able to remove content about him,

> I guess it depends on what it is, the nature of the… yeah there's been photographs that I really didn't think I wanted to ever see again and somebody else posted them up on behalf… it's just like… and sometimes you can get it removed and other times, it's not leaving. It's not going anywhere, so, whatever. What are you going to do about it?

When probed further on whether or not he had made attempts to report the content or delete it he replied:

> I talked to the person directly. And there's only so much some people can do about it, I don't know. "Once it's out there, it's out there" seems to be the mantra. You can try to put the genie back in the bottle but…

Again these responses illuminate this issue of desiring agency and autonomy over one's personal information within a digital context; Barney acknowledges his preference for control in shaping his virtual identity (through the removing of certain content online) however he acknowledges the sheer lack of power he has over making the changes he wants. This leads to the following responses that indicate an attitude of resignation: 'there's only so much some people can do about it' and 'it's not going anywhere, so what are you doing to do about it?' The acceptance of loss of control can lead some digital users to adopting a fatalistic-type response as a way of rationalizing the restrained effort they employ. When one feels as though they cannot make changes congruent with their

preferences it reduces self-efficacy, motivation, and optimism. The feeling that one must engage online to remain socially relevant in the current culture of surveillance amplifies the response of resignation as individuals feel constrained by normative forces built around the incorporation of digital technologies into everyday experience. Separating oneself from the digital can seem like social self-destruction for some, leading users to reluctantly maintain digital engagement just to stay involved and connected to established social ties.

Chapter 5

5

5.1 Discussion

The purpose of this study was to enrich the current discussion on privacy and how it is negotiated within the context of surveillance culture. In examining the privacy attitudes and behaviours of East Yorkers, this analysis illuminates the prevalence of resignation as an attitudinal response to the surveillance culture presently encountered. Though the response of each participant was unique based on their individual experiences, common themes did result from the analysis; these include: mistrust, perceived self-unimportance, loss of control, agency and resignation. In the following sections I will discuss these themes, situating their relevance within the broader literature. I will then address limitations of the present study and conclude with recommendations for further research.

Mistrust represented a common attitude shared among respondents. The nuances resulting from this theme led to it being divided up into five forms of mistrust including mistrust towards known others, unknown others, corporations, government and technological and online services. The model of social interaction as mediated through technology created complications for respondents in allowing themselves to trust contacts on their social media accounts. In such interactions the digital user looses full control of his or her information due to the networked structure of social media; privacy in such settings does not exist in a vacuum contained within the preferences of the individual user, rather it is a dynamic and negotiated process dependent on the people involved and the technology used. This is particularly relevant to feelings of mistrust towards *known others*; for respondents, concerns were expressed towards people they had on their social network accounts due to the access they had to their personal content. Some individuals expressed wariness about their contacts on their social media using their information against them. Linking this to the notion of loss of control, the acknowledgement that despite one's efforts to remove content online there remains a chance that it can be accessed and used by others amplified this sense of mistrust among respondents. This

suspicion towards the motives of other users lends credence to the theory of privacy cynicism. Hoffman, Lutz and Ranzini (2016) found that individuals universally expressed mistrust towards the motives of other people; participants doubted the intentions of other users online as well as agents shaping the online environment such as technology service providers. Believing that contacts on one's social media account and the owners of services being used are purely motivated by self-interest contributed to the manifestation of cynical thoughts regarding privacy and control among study participants. This doubt regarding the motives of others also applied to the theme of mistrust towards unknown others. Many respondents discussed their reservations with using public chats and open forums. In particular, the concern regarding the security of their identity was of primary importance when interacting with unknown others; respondents expressed wariness about their real identity being revealed and the dangers it would pose to them and their family.

The other forms of mistrust namely mistrust towards corporations, government and technological and online services all converge in interesting ways. These forms of mistrust were managed differently from mistrust towards people both known and unknown. Corporations, government and technological and online services represent institutional structures moulding our society, they shape and influence the ways in which we manage our daily lives. Engaging in any public space such as a mall, bank, sporting goods store or park introduces surveillance by government and corporate agents into our life. Utilizing social media, search engines such as Google, and online applications such as mobile banking, permit corporations and technological services to monitor our digital movements. With mistrust towards unknown and known others, respondents expressed more direct and tangible protection strategies online. For instance, individuals would avoid posting information on their social media or delete various contacts to protect themselves from people they knew online. Similarly in the case of mistrust towards unknown others, respondents would refrain from engaging in open forums or they would use aliases as an added form of identity protection when interacting online. Employing protective mechanisms against the surveillance practices carried out by government, corporations and technological services proved to be more complicated for respondents. The benefits made available through use of digital services made opting out from digital engagement a non-option for some. Further, though individuals could try to limit their

digital engagement, monitoring in the form of video and audio would still occur in public spaces, leading to this idea of inescapable surveillance. When discussing mistrust towards these institutions respondents would express their acknowledgement of the issue of vested interests. Corporations, government and technological services have a stake in the user providing personal information. Individuals were aware of this and expressed feeling a loss of control regarding data collection on behalf of these institutions. The surveillance practices employed by government and corporate forces make avoidance of being watched nearly impossible. In response, many individuals maintained use of technology despite understanding its potential application for monitoring because their routines were so strongly intertwined with use of digital technologies.

The main takeaway with the theme of mistrust is this notion that although respondents prefer to have control over their personal information, feelings of mistrust result from the acknowledgement of the lack of control they had. Thus, mistrust is highly weaved into feeling a loss of control; the combination of feeling a loss of control with feeling suspicious towards the motives of others results in a position of resignation in that individuals feel restrained in their ability to make real changes to the issues impacting and fuelling their sense of mistrust. As a result, they exercise resignation as a coping strategy to manage their feelings of mistrust in the very environment they perceive to be threatening their trust.

Next, the theme of perceived self-unimportance presented interesting points and accompanying consequences for individuals expressing this attitude towards their digital activity. There was a sense of naiveté in the participants' responses in that they believed they were simply uninteresting and therefore not worth monitoring. In some instances this led to reduced protection of personal information in that individuals believed their efforts to protect themselves were futile due to their perception that they and their information was unimportant and therefore not at risk. The notion that attention will be directed towards more high profile or high-alert individuals online brushes over the current state of surveillance: that each and every individual and their respective data equals value to data miners. This belief that one is an unimportant or uninteresting user caused some individuals to feel a sense of resignation towards collection of their data. Respondents rationalized their avoidance of concern over surveillance and data collection

through the attribution of themselves as being unimportant. Again we see here how resignation plays a key role in mediating how individuals who hold this self-perception respond to practices of data collection. This response has implications for the protection of data because subscribing to this attitude convinces the user that their data is not worth protecting. Though it can be difficult to completely avoid breaches to one's personal information online, efforts at protection of data are important nonetheless for they inform the services provided by technologies; if people want options to protect their data and the consumer need is great enough, corporations will make an effort to appease the members using their digital service in an effort to sustain the data-sharing relationship (Van Dijck, 2013). It is critical that individuals are informed of the value of their data concerning its uses in the digital market so that they are made aware of the potential consequences resulting from the assumption that no protection is a viable option.

A sense of loss of control was expressed by many respondents and tied all of the themes together representing an overarching feeling people experience in dealing with privacy in a digital and surveillance context. For digital users, loss of control was connected to the options or lack thereof that were provided by digital services. What a user can post, comment, like, tag, and report is based on the mechanisms and policies of the site in use. Put another way, digital services differ in the purpose of their platform and in the policies informing their platform, and these differences impact the experience of the user through the options afforded to them in using the service. For example, the social media site Facebook introduced a change to the like feature within their platform. Originally users were able to simply like another post on the site represented by a blue thumbs up icon. Now users are able to respond to a post with more options: Love, Haha, Wow, Angry, and Sad, each represented by a different symbol (Thielman, 2016). This example illustrates the influence a digital service can have on the users' experience based on the setup of the site; the user responds to and interacts with the site according to the options that are offered, in this way their agency and autonomy is constrained by these options. Another factor exacerbating feelings of loss of control was the frequent changes to privacy policies by digital services, these policies are detailed in Terms of Service (ToS) and End User License Agreements (EULAs).

Respondents expressed frustration over changes to policies such as the ToS and EULA, again reinforcing the reality of reduced control they believe they faced. Users' knowledge of the digital service they are using is based off of the ToS and EULA they agree to when they first sign up to use the digital service. When these policies are changed users expect to be notified however this does not always occur, as was exemplified in the previous example regarding changes to Facebook's policy in 2010 (Keys, 2018). The knowledge that users have regarding how the digital service stores and uses their personal information is based off of the ToS and EULA they initially sign when they begin use of the service. Not being notified when pertinent changes to these policies occur reinforces feelings of mistrust and loss of control on behalf of digital users.

In understanding that databases storing personal information could be breached and hacking could occur, respondents were also aware that their data could be misused. Based on this they discussed their unease regarding the flow of their data, admitting that not knowing where their data was going or to whom it was being sold caused anxiety. This lack of awareness combined with an understanding of technology as dynamic and evolving, caused respondents to feel a loss of control over their personal data. There was a sense that engagement with digital technologies inevitably and unavoidably brings with it a loss of control. To reconcile their desire for control with the reality of diminished control they faced, some individuals would respond with resignation towards practices of data protection.

Recognition of reduced control did not mean unfettered acceptance of the state of things; respondents did express a desire for control and some exercised various strategies in an attempt to protect their personal information when using digital services. Indeed, other studies have shown control to be extremely important for individuals in digital contexts. In researching online privacy, Turow (2003) found that Americans do want help in controlling their information online and 95% agreed that they should have a legal right to know everything a website knows about them. In more recent work, 84% of Americans agreed that they want to have control over what marketers could learn about them however 65% accepted that they had little control over what marketers could learn about them online (Turow, Hennessey and Draper, 2015). Although individuals desire control, they become resigned to the reality of limited control. In the next section I will address

the theme of agency and how respondents in East York actively made attempts to gain control over their data despite the obstacles they describe.

Respondents in this sample did make attempts to gain agency over their personal data and digital interactions. An important note about agency in this study was that although respondents did exert various strategies to protect themselves online they did so while acknowledging their reduced control. In understanding the restraints to control faced within digital environments, users framed their protective behaviours in response to this context. Some of the obstacles described by respondents in exerting control over their personal information online consisted of: frequent changes to privacy policies and limited options provided by social media sites and digital applications. As mentioned earlier, the ability for a user to control their data (what they share, to whom they share it, and what privacy controls they impose on it) is based on the affordances permitted by the service in use. This makes the exertion of agency dependent on the bounds set by the service in use. One respondent was unhappy about the security options provided by the social media site Facebook so in response he deactivated his account, opting out from use. However he had access to his work Facebook account so he was able to subjugate these restrictions and continue use of the site through an impersonal account. This example illuminates the agency a user can have in avoiding use of social media; one can opt out entirely, ultimately removing themselves from the constant nag of notifications and potential risks to privacy but social repercussions can result making complete avoidance of social media unattainable for some. Still, the above respondent's effort to use another Facebook account to accommodate his issues with Facebook's security policy does represent an agentic response to the restrictions he faced in this case.

Other respondents in this sample would voluntarily share their personal information acting agentically in this regard, however they were clear about the boundaries regarding what they were and weren't comfortable with. Remaining anonymous was important for some and maintenance of confidentiality helped to perpetuate their engagement with digital technologies. Further, respondents were aware that information kept from digital settings guaranteed a kind of protection, motivating them to be cautious about what content they themselves and others posted about them on their social media accounts. Numerous respondents brought up the issue of employers

being able to search one's digital history leading to potential complications in securing occupational positions; from this, some made mention of their efforts to reduce these risks by removing unflattering or disturbing content posted about them online. Even here, under the theme of agency, links to a loss of control are recognized. Despite the efforts of some to remove content posted about them online, they understood their agency was limited. Information posted about them could remain public in spite of their complaints to remove it; illuminating again the fact that agency can be exerted however the results may not align with the respondent's desired outcomes. Respondents made clear their awareness of the limits to their agency yet attempts to gain control were worthwhile for them. Indeed despite the possibility that data can always be compromised, the utilization of privacy protective behaviours helped to alleviate pressing privacy concerns for some, making their efforts valuable to them.

The final and perhaps most prevalent theme resulting from this analysis is resignation. The discussion of surveillance culture in previous sections of this paper was intended to illustrate the pervasive nature of surveillance in North American and Western European society. The interaction between digital technologies and practices of self-surveillance and surveillance of others has incorporated the experience of monitoring and being monitored into everyday life. As discussed in previous sections of this paper, complete avoidance of surveillance is not feasible; public movements are watched, phone calls can be accessed and so on. Considering this, it is unsurprising then that individuals come to accept surveillance in some form, as life in our modern materialistic age is unrealistic without it. However what is interesting is the voluntary participation of individuals in their own surveillance through engagement with digital applications and technologies. The normalization of use of these technologies in daily routines has caused individuals to feel as though there is no alternative reality to the current surveillance culture. This is where surveillance realism comes in, that individuals become resigned to the undesirable characteristics of surveillance due to their feeling that there is no alternative available to them. The predominance of surveillance by virtue of engagement with digital technologies is one aspect that has contributed to the response of digital resignation. Another issue, expressed by respondents in this study, connects to the theme of loss of control.

Digital users are largely uninformed regarding the flow of their digital data and this negatively impacts the individual's ability to gain greater understanding of the risks involved with use of various sites and technologies (see Viseu et al., 2004). Digital users can agree to use a site based on a particular privacy policy however this policy can change and sometimes the affected users are left untold. This lack of control over the decisions that technology providers make regarding the data they possess can cause individuals to feel restrained in their agency, feeling virtually powerless over what happens to their personal information. Respondents in this sample were aware of this and understood that despite their efforts aimed at protection of their information, breaches could still occur. This restrained ability to be fully in control or aware of what is happening to one's data also contributed to digital users feeling resigned.

As illustrated in the above paragraphs, lack of control and practices of surveillance have become intrinsic to engagement with digital technologies. The incorporation of these digital technologies into everyday routines has as a result, normalized the experience of lack of control and surveillance. In responding to this climate, the position of resignation allows individuals to retain their preference for privacy despite this need not being met in their current situation. The concepts of security fatigue and privacy fatigue describe the condition of exhaustion that occurs when one cannot achieve their desired needs amidst the borage of messages encouraging control and privacy. This lack of achievement can lead to decreased self-efficacy and cognitive incongruence. Adopting a stance of resignation allows one to have a sense of control; that the realization they lack control gives them assurance that their efforts to completely protect themselves are unrealistic as per the unequal power arrangement between user and technology provider. This position of resignation, as a response to the prospect of attaining control in digital spaces, allows users to cope with their privacy concerns while remaining engaged with various technologies. When control is desired but cannot be guaranteed or achieved in a satisfactory manner, individuals accept these limitations in order to stay digitally connected. Choosing to be resigned to conditions that are completely out of one's control represents an astute cost-benefit analysis on behalf of users; indeed this type of response is rational in that individuals actively manage the ways in which they have control and lack control through their efforts to protect themselves

online. The responses of study participants exemplify this point in that they recognize the options available to them that allow them to protect themselves online however these efforts by no means guarantee complete and continuous protection.

Criticism has been directed against the idea of resignation as a form of privacy response, with proponents of this position ascribing digital resignation to passive digital users who willfully submit to the actions of technology providers (Lyons, 2018). However the paradigm of digital resignation represents quite the opposite; individuals are viewed as rational and capable digital users. However, with limited awareness of the actual mechanics behind the technologies and services they use and restrained knowledge regarding the movement of their data, digital users resort to coping with the constraints to their privacy through resignation. The response of resignation is rational indeed as it permits concerns regarding data collection and privacy related-issues to exist while simultaneously allowing individuals to remain digitally connected despite these. Efforts to opt out of social media and other online services can and do happen but individual users who drop out often return (Draper & Turow, 2019). Indeed collective movements campaigning changes to prohibitive or exploitative policies can occur, nevertheless the reigns of control overwhelmingly remain in the hands of the owners of technological services. The success of efforts at widespread resistance towards surveillance and data collection are dependent on legislative involvement or collective empowerment and the individual actions of digital users infrequently aggregate to foster the systemic changes needed (Draper & Turow, 2019). This reinforces recognition of the position of resignation as a rational response: even if individuals decide to opt out, potentially experiencing social repercussions as a result, their efforts will likely have no impact on the direct issues that led them to end engagement. Resignation allows the digital user to maintain hold of and cope with his or her privacy-related concerns, while continuing engagement with digital and online technology. Individuals respond to the options available to them by either engaging in privacy protective behaviours or not, while also understanding in the same sense that these mechanisms may not guarantee any protection at all.

This study supports the sociology of digital resignation and provides new insights regarding the role of agency and perceived self-unimportance in relation to resignation.

The decision to include agency as a primary theme in this paper is to acknowledge the importance of users' attempts to negotiate and manage privacy in connection to the digital services in which they are engaged. Examples of agency are noted throughout in an effort to highlight the autonomy of digital users despite the limitations they face in using digital services (e.g. changing privacy policies, evolving technology, and limited site options). Important to note is the tenacity of users' to conform the services they use to their privacy preferences within digital settings; the lack of power and control confronting users does not bankrupt them of their desire for privacy, instead they diligently pursue other means to gain control such as refraining from posting information online, using impersonal social network accounts, and instituting settings to meet their privacy and social needs. Further research is needed to explore the connection between agency, loss of control and resignation within digital contexts in order to clarify the ways in which individuals manage the limitations they encounter in using digital services.

As for the theme of perceived self-unimportance, the findings in this study support other studies that have found evidence for this attitude (Stanton et al., 2016; Madden, 2015; Viseu et al., 2004). This type of stance is different from the position of resignation described throughout this paper in that the users with this attitude do not necessarily value or desire privacy. In the other themes privacy is an important value and digital users make consistent efforts to gain control; it is their realization regarding the limits to their agency that causes them to feel resigned. Regarding the attitude of perceived self-unimportance, these individuals do not necessarily indicate a great concern over their privacy, rather they contend that privacy protection is pointless because of the irrelevance of their data. When individuals feel as though they are uninteresting or unimportant, they have decreased regard for how their digital information will be used. For some digital users, the idea that their data has nothing fascinating or appealing to offer can result in weakened efforts at privacy protection. It can lead to a type of fatalism whereby the user feels that privacy protection is futile as their data lacks the importance needed to warrant protection. The connection between this attitude and resignation needs to be explored in order to investigate whether or not this attitude is a form of resignation, in that users become disengaged from efforts at protection of privacy.

5.2 Implications of Digital Resignation

It is important to consider the implications of digital resignation; is this a sustainable response to privacy related issues encountered online? If not, then what can consumers do to combat the seeming fatalistic response that resignation can engender?

The widespread use of technology among consumers has enabled large multi-national corporations and technological conglomerates to gain monopolizing power over the control of digital information. Shoshana Zuboff, a professor at the Harvard Business School, argues in her work on 'surveillance capitalism,' that large technology companies that have mass amounts of capital and power as a result of their collection of consumer's data, have been able to subvert principles fundamental to any democratic system: freedom, self-determination, autonomy, and human agency (Zuboff, 2019). Their efforts of monitoring have shifted towards aims of actualization; behavioural data is now collected in order to predict and shape the user's behaviours. This move towards actualization is also a move towards certainty; when a company can collect your data, make inferences, predict what you will do, and manipulate you into making decisions, they infer with increasing certainty how you will act in a range of situations. This eliminates the prospect of free will in that it undermines the wild and spontaneous nature of human agency. This is an attack on privacy and freewill.

Adding to this is the unequal power dynamic regarding the issue of knowledge; consumers have little to no knowledge of processes relevant to their data, while the corporation holds exhaustive knowledge of the consumer. This arrangement is disturbingly unequal and is shaping the way digital privacy is negotiated and managed. When consumers feel they lack the clout needed to change business or government policy with regard to the treatment of their personal information (digital or not), feelings of resignation can result which as shown throughout this paper, can cause users to become disengaged from efforts of privacy protection. Further, resignation as a response to privacy-related concerns actually benefits corporate interests. Draper and Turow (2019) discuss how corporate and digital media firms work to actively discourage collective resistance against media (Draper & Turow, 2019). Resignation can produce feelings of futility and helplessness on the part of the user which in turn, benefits the corporate

agenda as they are able to maintain routine practices of data collection, aggregation, and computation, despite consumers airing concerns regarding the security and privacy of their digital data. In order to combat the cultivation of resignation observed in digital spaces, fundamental democratic values need to be acknowledged in this discussion. Privacy is one of these values; the narrative around privacy suggests that it is a personal process, one which includes a decision to engage or not; to provide information or not. A consequence of resignation for the individual is a turning inward of privacy and surveillance concerns (Draper & Turow, 2019). However privacy is social; it is societal and therefore, a collective action problem. We solve collective action problems with law and through the principles of democracy.

Zuboff (2019) maintains that a primary way to tackle this system of unequal information and knowledge control is through the involvement of government and democratic institutions. What tech companies fear is legislation; lawmakers need to embark on a mission of resurrecting the digital for good, of resurrecting the democratizing functions of technology for users and institutions alike. One way in which technology companies have been able to become powerful is through the unencumbered collection and selling of user's personal information. Interruption of the flow of data and accompanying revenue is an initial step towards prohibiting the recording of personal information. Lawmakers can also encourage citizens towards alternative forms of collective action; citizens need the support of their elected officials to institute change at legislative levels and once this occurs, the necessary shift in public opinion will be possible. Alternative forms of resistance are actively being explored in current discussions regarding these issues. One such focus has been on how social media platforms and technology services can be democratized. Is it possible to turn major platforms like Facebook and Twitter into public or government utilities, resembling National Public Radio (NPR) or the Canadian Broadcasting Corporation (CBC)? Another idea put forth has been turning these same large platforms into digital cooperatives, where the company is owned by users through shares and where tax funds could maintain the technical aspects of the system. These ideas to democratize social media and technology services are at the level of infancy and therefore require development,

however, this exploration is critical at a time where the bounds of information control and therefore freedom, are being actively negotiated and grappled with.

5.3 Limitations

Digital technologies develop at a frequent pace leading to changes in how citizens navigate use of these services. For this reason, findings from this analysis may need to be revisited and updated in order to investigate their application to variable contexts. Further, the cross-sectional design of this study does not allow us to examine changes to privacy attitudes and concerns that occur over time therefore limiting our ability to examine how these study participants have been affected by the introduction of new technologies and privacy issues. Future research could pursue longitudinal analysis to examine how privacy attitudes and behaviours change based on the dynamic digital environment. Another possible limitation of this study is a methodological one. The interviewers who worked closely with the study participants were internet-savvy university students (aged 25-30 years). The younger age range comprising the researchers involved in the interviewing process could have affected older adults' self-assessment of their digital skills. Finally, due to limits in time and the overall scope of this study further probing of respondents' answers was not feasible.

5.4 Contributions and Directions for Future Research

The introduction of digital resignation to debates covering issues of security, privacy and surveillance has opened up the conversation, allowing consideration of new forms of response to privacy issues within a surveillant context. Previous research has commented on the inaction of the public to institute privacy protection online (Draper, 2017; Hargittai & Marwick, 2016). This has resulted in a mass of research directed towards investigating the attitude-behaviour disconnect (see Kokolakis, 2017). That is, where people express a desire for privacy while at the same time avoiding use of privacy protection to achieve said desire. This represents what academics refer to as the "privacy paradox" however few studies have investigated alternative explanations of this discrepancy. This study supports the emerging and rich body of research on the sociology of resignation and its application as a response to said discrepancy. The findings put forth in this paper are congruent with other studies that have examined resignation within a

digital context. Further, this study is the first to investigate the prevalence of digital resignation from a Canadian context, offering support in the way of its generalizability to other regions.

The resulting themes of loss of control, mistrust and resignation that comprise this analysis echo findings from recent research, adding to what we currently know about resignation (Turow, 2003; Turow, Hennessy & Draper, 2015; Hargittai & Marwick, 2016; Hoffman, Lutz & Ranzini, 2016; Draper, 2017; Draper & Turow, 2019; Dencik & Cable, 2017). The themes of agency and perceived self-unimportance as reviewed in this analysis offer insights into new areas of research worth pursuing. As discussed, being resigned does not indicate a complete avoidance of efforts to protect oneself online; indeed digital users still make attempts to shield themselves from digital threats, however they feel these efforts may not be successful. The position of resignation is not one of apathy; people maintain concern over their personal information online and make attempts to protect it, however they do so with the recognition that these attempts may be unsuccessful and therefore futile. The relationship between agency and resignation can be investigated further to understand more deeply the negotiation that occurs between desire and exertion of agency amidst loss of control and uncertainty in digital contexts. Additionally, the connection between perceived self-unimportance and resignation is also an area of scholarship worth pursuing in order to clarify how the two concepts intersect and whether or not the attitude of perceived self-unimportance can be viewed as a form of resignation.

5.2 Conclusion

This research contributes to the literature by providing support for the application of resignation as a form of response to privacy, security and surveillance issues faced within digital environments. The aim of this study was to examine the privacy-related attitudes and experiences of East Yorkers in their use of digital services. Based on analysis of in-depth semi-structured interviews, participants in this sample were able to provide rich insight on how they manage privacy and security within digital environments. The responses indicated by East Yorkers reflect those found in other qualitative data. Specifically, the theme of loss of control or powerless as put in other

studies (Lutz, Hoffman & Ranzini, 2016) has been shown to be a predominant response in navigating digital spaces, eventually leading to or contributing towards feeling resigned. Feelings of mistrust towards government and corporate entities have also been noted in the literature (Madden, 2014; Turow, 2003).

As discussed previously in this paper, privacy attitude is frequently used to predict privacy behaviour. However the association between attitude and behaviour has been shown to be weak and only predictive when distinct privacy attitudes are used (Dienlin & Trepte, 2015; Kokolakis, 2017). The findings in this study support the adoption and application of resignation as an explanation to the attitude-behaviour disconnect, labelled as "the privacy paradox". This paper argues for examination of the above paradox in terms of resignation; this opens up the limiting association connecting privacy attitudes to behaviours and allows for new considerations to be pursued. Resignation offers a unique model for understanding the problem of privacy and how it is managed in digital environments. The privacy paradox model that infers an informed and empowered consumer, aware of all possible risks and consequences to his or her data, is informed primarily by responsibility and choice. However digital users feel a loss of control due to the limited choice available to them and they experience resignation because they feel restricted in their ability to be informed. Recognition of this needs to be taken into account when discussing digital privacy in order to enhance the conversation around the rights and responsibilities attributed to digital users.

Changing the script that is focused on the informed and in-control digital user can facilitate a revaluation of policy, mandating firms to reassess the position of the empowered consumer at the center of their business models. Such a shift can positively redirect the burden of responsibility previously assumed by consumers to the corporations providing digital services. The implications of using data, which is provided primarily by uninformed digital users, needs to be seriously considered as the databases storing big data are perpetually at risk of being breached. As such, the onus of responsibility needs to be directed towards organizations and corporations through legislation; though this will not solve problems of digital privacy, it can contribute to a changed digital environment marked by accountability of both the digital user and digital provider.

References

Abbate, J. (2017). What and where is the internet? (re)defining internet histories. *Internet Histories*, 1(1-2), 8-14. doi:10.1080/24701475.2017.1305836

Acquisti, A., & Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the Facebook. (pp. 36-58). Berlin, Heidelberg: Springer Berlin Heidelberg. doi:10.1007/11957454_3

Adela, N., & Diana, R. (2018). Determinants of housing prices: Evidence from Ontario cities, 2001-2011. *International Journal of Housing Markets and Analysis,* 11(3), 541-556. doi:http://dx.doi.org/10.1108/IJHMA-08-2017-0078

Afroz, S., Islam, A. C., Santell, J., Chapin, A., & Greenstadt, R. (2013). How Privacy Flaws Affect Consumer Perception. 2013 Third Workshop on Socio-Technical Aspects in Security and Trust. doi:10.1109/stast.2013.13

Aharony, N. (2016). Relationships among attachment theory, social capital perspective, personality characteristics, and Facebook self-disclosure. *Aslib Journal of Information Management*, 68(3), 362-386. doi:10.1108/AJIM-01-2016-0001

Altman, I. (1975). *The environment and social behavior: Privacy, personal space, territory, crowding*. Monterey, CA: Brooks/Cole Pub. Co.

Anderson, M., & Perrin, A. (2017). *Tech Adoption Climbs Among Older Adults*. Pew Research Center. http://www.pewinternet.org/2017/05/17/tech-adoption-climbs-among-older-adults/ Accessed 16 August 2018

Ando, H., Cousins, R., & Young, C. (2014). Achieving saturation in thematic analysis: Development and refinement of a Codebook1,2,3. *Comprehensive Psychology,* 3 doi:10.2466/03.CP.3.4

Bansal, G., Zahedi, F. M., & Gefen, D. (2016). Do context and personality matter? trust and privacy concerns in disclosing private information online. *Information & Management,* 53(1), 1-21. doi:10.1016/j.im.2015.08.001

Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday*, 11(9). http://firstmonday.org/issues/issue11_9/barnes/index.html/ Accessed 08.01.18]

Bartsch, M., & Dienlin, T. (2016). Control your facebook: An analysis of online privacy literacy. *Computers in Human Behavior*, 56, 147-154. doi:10.1016/j.chb.2015.11.022

Bergström, A., Institutionen för journalistik, medier och kommunikation (JMG), Department of Journalism, Media and Communication (JMG), Göteborgs universitet, Gothenburg University, Samhällsvetenskapliga fakulteten, & Faculty of Social Sciences. (2015). Online privacy concerns: A broad approach to

understanding the concerns of different groups for different uses. *Computers in Human Behavior*, 53, 419-426. doi:10.1016/j.chb.2015.07.025

Brailovskaia, J., & Margraf, J. (2016). Comparing facebook users and facebook non-users: Relationship between personality traits and mental health variables - an exploratory study. *PloS One*, 11(12), e0166999. doi:10.1371/journal.pone.0166999

Brake, D. (2014). *Sharing our lives online: Risks and exposure in social media.* Basingstoke, Hampshire: Palgrave Macmillan.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101. doi:10.1191/1478088706qp063oa

Braun, V., & Clarke, V. (2013). Successful qualitative research: A practical guide for beginners. London: SAGE.

Brown B. Studying the internet experience. HP Laboratories Technical Report (HPL-2001-49). <http://www.hpl.hp.com/ techreports/2001/HPL-2001-49.pdf>; 2001/ Accessed 07.24.18].

Burgoon, J. K. (1982) Privacy and communication. Beverly Hills: Burgoon, M. (ed.), Communication Yearbook 6.

Chang, M. K., Cheung, W., & Tang, M. (2013). Building trust online: Interactions among trust building mechanisms. *Information & Managemen*t, 50(7), 439-445. doi:10.l1016/j.im.2013.06.003

Chayko, M. (2016). *Superconnected: The internet, digital media, and techno-social life*. Los Angeles: SAGE.

Chen, H. (2018). Revisiting the privacy paradox on social media with an extended privacy calculus model: The effect of privacy concerns, privacy self-efficacy, and social capital on privacy management. *American Behavioral Scientist*, 62(10), 1392-1412. doi:10.1177/0002764218792691

Chesley, N., & Fox, B. (2012). E-mail's use and perceived effect on family relationship quality: Variations by gender and Race/Ethnicity. *Sociological Focus*, 45(1), 63-84. doi:10.1080/00380237.2012.630906

Choi, H., Park, J., & Jung, Y. (2018). The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81, 42-51. doi:10.1016/j.chb.2017.12.001

City of Toronto. (2019, May 08). Toronto at a Glance. Retrieved from https://www.toronto.ca/city-government/data-research-maps/toronto-at-a-glance/

Clarke, R. (1997). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. Retrieved August 4, 2018, from http://www.rogerclarke.com/DV/Intro.html

CREA (2011) Housing Market Outlook: Ontario Region Highlights, Canada Mortgage and Housing Corporation. Available at: http://publications.gc.ca/collections/collection_2011/schl-cmhc/nh12-262/NH12-262-4-2011-2-eng.pdf

Debatin, B., Lovejoy, J. P., Horn, A., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 15(1), 83-108. doi:10.1111/j.1083-6101.2009.01494.x

Dencik, L., & Cable, J. (2017). The advent of surveillance realism: Public opinion and activist responses to the snowden leaks. *International Journal of Communication*, 11, 763-781.

Dienlin, T., & Trepte, S. (2015). Is the privacy paradox a relic of the past? an in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, 45(3), 285-297. doi:10.1002/ejsp.2049

Dijck, J. v. (2013). *The culture of connectivity: A critical history of social media.* New York;Oxford;: Oxford University Press.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, 22(3), 295-316. doi:10.1057/ejis.2012.23

Draper, N. A. (2017). From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates: Challenging rational choice in digital privacy debates. Policy & Internet, 9(2), 232-251. doi:10.1002/poi3.142

Draper, N. A., & Turow, J. (2019). The corporate cultivation of digital resignation. *New Media & Society*, 21(8), 1824-1839. doi:10.1177/1461444819833331

Dunning, D. (n.d.). What Is Digital Technology? Retrieved June 20, 2019, from https://www.techwalla.com/articles/what-is-digital-technology.

Elueze, I., & Quan-Haase, A. (2018). Privacy attitudes and concerns in the digital lives of older adults: Westin's privacy attitude typology revisited. *American Behavioral Scientist*, 62(10), 1372-1391. doi:10.1177/0002764218787026

Ferreira, S. M., Sayago, S., & Blat, J. (2017). Older people's production and appropriation of digital videos: An ethnographic study. *Behaviour &*

Information Technology, 36(6), 557-574. doi:10.1080/0144929X.2016.1265150

Fidler, D. P., & Ganguly, S. (2015). *The Snowden Reader.* Bloomington, Indiana]; Indiana University Press.

Fisher, M. (2009). *Capitalist realism: Is there no alternative?* Washington, D.C.;Winchester, UK; Zero Books.

Finn, R. L., Wright, D., & Friedewald, M. (2013). Seven types of privacy. doi:10.1007/978-94-007-5170-5_1

Gatto, S. L., & Tak, S. H. (2008). Computer, internet, and E-mail use among older adults: Benefits and barriers. *Educational Gerontology*, 34(9), 800-811. doi:10.1080/03601270802243697

Groes, S. (2017). Information overload in literature. *Textual Practice*, 31(7), 1481-1508. doi:10.1080/0950236X.2015.1126630

Gross, R., & Acquisti, A. (2005). Information revelation and privacy in online social networks. Paper presented at the 71-80. doi:10.1145/1102199.1102214

Hargittai, E., & Marwick, A. (2016). "what can I really do?" explaining the privacy paradox with online apathy. *International Journal of Communication* (Online), 3737.

Hevner, A., Chatterjee, S. (2010). Design research in information systems: Theory and practice. Boston, MA: *Springer Science+Business Media*, LLC.

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. (2019). *Digital citizenship in a datafied society*. Cambridge, UK;Medford, MA, USA;: Polity Press.

Hoffman, C. P., Lutz, C., & Ranzini, G. (2016). Privacy cynicism: A new approach to the privacy paradox. Cyberpsychology: *Journal of Psychosocial Research in Cyberspace* (Online), 10(4) doi:10.5817/CP2016-4-7

Hoofnagle, C. J., King, J., Li, S., & Turow, J. (2010). How Different are Young Adults from Older Adults When it Comes to Information Privacy Attitudes and Policies? http://dx.doi.org/10.2139/ssrn.1589864

Hoofnagle, C. J., & Urban, J. M. (2014). Alan Westin's privacy homo economicus. *Wake Forest Law Review*, 49(2), 261.

Ivan, L., & Hebblethwaite, S. (2016). Grannies on the net: Grandmothers' experiences of facebook in family communication. Revista Română De Comunicare Şi Relaţii Publice, 18(1), 11-25. doi:10.21018/rjcpr.2016.1.199

Jeong, Y., & Kim, Y. (2017). Privacy concerns on social networking sites: Interplay among posting types, content, and audiences. *Computers in Human Behavior*, 69, 302-310. doi:10.1016/j.chb.2016.12.042

Karsten, J., & West, D. M. (2016). Terrifying technology tops list of American fears. Retrieved from https://www.brookings.edu/blog/techtank/2015/10/30/terrifying-technology-tops-list-of-american-fears/

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). *Thinking Styles and Privacy Decisions: Need for Cognition, Faith into Intuition, and the Privacy Calculus*.

Kehr, F., Kowatsch, T., Wentzel, D., & Fleisch, E. (2015). Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, 25(6), 607-635. doi:10.1111/isj.12062

Keys, Matthew. (2018). A brief history of Facebook's ever-changing privacy settings. Retrieved from https://medium.com/@matthewkeys/a-brief-history-of-facebooks-ever-changing-privacy-settings-8167dadd3bd0

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security*, 64, 122-134. doi:10.1016/j.cose.2015.07.002

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of Information Technology*, 25(2), 109-125. doi:10.1057/jit.2010.6

Lanier, C. D., Jr, & Saini, A. (2008). Understanding consumer privacy: A review and future directions. *Academy of Marketing Science Review*, 2008, 1.

Liu, Y., Gummadi, K., Krishnamurthy, B., & Mislove, A. (2011). Analyzing Facebook privacy settings: User expectations vs. reality. Paper presented at the 61-70. doi:10.1145/2068816.2068823

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: Teenagers' use of social networking sites for intimacy, privacy and self-expression. *New Media & Society*, 10(3), 393-411. doi:10.1177/1461444808089415

Lovink, G., & Rasch, M. (2013). *Unlike us reader: Social media monopolies and their alternatives*. Amsterdam: Institute of Network Cultures.

Lupton, D. (2015). *Digital sociology*. Abingdon, Oxon: Routledge.

Lupton, D. (2016). *The quantified self: A sociology of self-tracking*. Cambridge, UK;Malden, MA;: Polity.

Lyon, D. (2017). Surveillance culture: Engagement, exposure, and ethics in digital modernity. *International Journal of Communication* (Online), 824.

Madden, M. (2014). *Public Perceptions of Privacy and Security in the Post-Snowden Era.* Pew Research Center. https://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ Accessed 03 June 2019

Madden, M., & L. Raine. (2015). *Americans' Attitudes About Privacy, Security, and Surveillance.* Pew Research Center. http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ Accessed 02 June 2019

Manning, J. (2014). Social media, definition and classes of.

Martin, K., & Shilton, K. (2016). Why experience matters to privacy: How context-based experience moderates consumer privacy expectations for mobile applications. *Journal of the Association for Information Science and Technology*, 67(8), 1871-1882. doi:10.1002/asi.23500

Mary Jane Kwok Choon. (2018). Revisiting the privacy paradox on social media: An analysis of privacy practices associated with Facebook and Twitter. *Canadian Journal of Communication*, 43(2), 339-358. doi:10.22230/cjc.2018v43n2a3267

Mok, D., Wellman, B., & Carrasco, J. (2010). Does distance matter in the age of the internet? *Urban Studies*, 47(13), 2747-2783. doi:10.1177/0042098010377363

Moloney, M., & Bannister, F. (2009). A privacy control theory for online environments. Paper presented at the 1-10. doi:10.1109/HICSS.2009.31

Nistor, A., & Reianu, D. (2018). Determinants of housing prices: Evidence from ontario cities, 2001-2011. *International Journal of Housing Markets and Analysis*, 11(3), 541-556. doi:10.1108/IJHMA-08-2017-0078

Obar, J. A., & Wildman, S. (2015). Social media definition and the governance challenge: An introduction to the special issue. *Telecommunications Policy*, 39(9), 745-750. doi:10.1016/j.telpol.2015.07.014

Oestreicher, K. (2014). A forensically robust method for acquisition of iCloud data. *Digital Investigation,* 11, S106-S113. doi:10.1016/j.diin.2014.05.006

Office of the Privacy Commissioner of Canada. (2016, December). 2016 Survey of Canadians on Privacy. Retrieved May 20, 2019, from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/#fig20

Pierson, J., & Heyman, R. (2011). Social media and cookies: Challenges for online privacy. Info, 13(6), 30-42. doi:10.1108/14636691111174243

Plickert, G., Côté, R. R., & Wellman, B. (2007). It's not who you know, it's how you know them: Who exchanges what with whom? *Social Networks*, 29(3), 405-429. doi:10.1016/j.socnet.2007.01.007

Purcell, P. (2006). Networked neighbourhoods: The connected community in context. London, UK: Springer. doi:10.1007/1-84628-601-8

Quan-Haase, A., & Elueze, I. (2018). Revisiting the privacy paradox: Concerns and protection strategies in the social media experiences of older adults. Paper presented at the 150-159. doi:10.1145/3217804.3217907

Quan-Haase, A., Martin, K., & Schreurs, K. (2016). Interviews with digital seniors: ICT use in the context of everyday life. *Information, Communication & Society*, 19(5), 691-707. doi:10.1080/1369118X.2016.1140217

Quan-Haase, A., Mo, G. Y., & Wellman, B. (2017). Connected seniors: How older adults in East York exchange social support online and offline. *Information, Communication & Society*, 20(7), 967-983. doi:10.1080/1369118X.2017.1305428

Quan-Haase, A., Williams, C., Kicevski, M., Elueze, I., & Wellman, B. (2018). Dividing the grey divide: Deconstructing myths about older adults' online activities, skills, and attitudes. *American Behavioral Scientist*, 62(9), 1207-1228. doi:10.1177/0002764218777572

Rainie, L., & Anderson, J. (2014). *The Future of Privacy*. Retrieved from https://www.pewinternet.org/2014/12/18/future-of-privacy/

Rainie, L., Keeter, S., & Perrin, A. (2019). *Americans' Trust in Government, Each Other, Leaders*. Pew Research Center. https://www.people-press.org/2019/07/22/trust-and-distrust-in-america/ Accessed 28 July 2019

Rainie, L., & Madden, M. (2015). Americans' Privacy Strategies Post-Snowden. Retrieved from https://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/

Rainie, H., & Wellman, B. (2014). *Networked: The new social operating system.* Cambridge: MIT Press.

Raynes-Goldie, K. (2010). Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, 15(1). http://dx.doi.org/10.5210/fm.v15i12775

Rule, J. B. (2007). *Privacy in peril*. New York: Oxford University Press.

Sajić, M., Bundalo, D., Bundalo, Z., & Pašalić, D. (2018). using digital and mobile technologies for increasing efficiency of financial institutions. *Acta Technica Corviniensis* - Bulletin of Engineering, 11(3), 39-42.

Schreurs, K., Quan-Haase, A., & Martin, K. (2017). Problematizing the digital literacy paradox in the context of older adults' ICT use: Aging, media discourse, and self-determination. *Canadian Journal of Communication*, 42(2), 359-377. doi:10.22230/cjc.2017v42n2a3130

Shane-Simpson, C., Manago, A., Gaggi, N., & Gillespie-Lynch, K. (2018). Why do college students prefer Facebook, Twitter, or Instagram? Site affordances, tensions between privacy and self-expression, and implications for social capital. *Computers in Human Behavior*, 86, 276-288. doi:10.1016/j.chb.2018.04.041

Sheehan, K. B. (2002). Toward a typology of internet users and online privacy concerns. *The Information Society, 18(1), 21-32. doi:10.1080/01972240252818207*

Simanowski, R. (2018). Facebook society: Losing ourselves in sharing ourselves. New York: Columbia University Press.

Sipior, J. C., Ward, B. T., & Mendoza, R. A. (2011). Online privacy concerns associated with cookies, flash cookies, and web beacons. *Journal of Internet Commerce*, 10(1), 1-16. doi:10.1080/15332861.2011.558454

Sivarajah, U., Irani, Z., & Weerakkody, V. (2015). Evaluating the use and impact of web 2.0 technologies in local government. *Government Information Quarterly*, 32(4), 473-487. doi:10.1016/j.giq.2015.06.004

Smith, A. (2017). *Americans and Cybersecurity.* Pew Research Center. https://www.pewinternet.org/2017/01/26/americans-and-cybersecurity/ Accessed 05 June 2019

Smith, S. (2015). How Americans view government: 6 key takeaways. Retrieved from https://www.pewresearch.org/fact-tank/2015/11/23/6-key-takeaways-about-how-americans-view-their-government/ Accessed 05 June 2019

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477-564. doi:10.2307/40041279

Stanton, B., Theofanos, M. F., Prettyman, S. S., & Furman, S. (2016). Security fatigue. *IT Professional*, 18(5), 26-32. doi:10.1109/MITP.2016.84

Steijn, W. M. P. (2014). A developmental perspective regarding the behaviour of adolescents, young adults, and adults on social network sites. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 8(2) doi:10.5817/CP2014-2-5

Steijn, W., Schouten, A. P., & Vedder, A. (2016). Why concern regarding privacy differs: The influence of age and non-participation on Facebook. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(1) doi:10.5817/CP2016-1-3

Steijn, W. M. P., & Vedder, A. H. (2015). Privacy under construction: A developmental perspective on privacy perception. *Science, Technology & Human Values*, 40(4), 615-637. doi:10.1177/0162243915571167

Stutzman, F., Vitak, J., Ellison N., Gray R., & Lampe, C. (2012). *Privacy in Interaction: Exploring Disclosure and Social Capital in Facebook.*

Symantec (2015). *State of privacy report 2015.* Symantec. http://www.symantec.com/content/en/us/about/presskits/b-state-of-privacy-report-2015.pdf/ Accessed 01 August 2018.

Taddei, S., & Contena, B. (2013). Privacy, trust and control: Which relationships with online self-disclosure? *Computers in Human Behavior*, 29(3), 821-826. doi:10.1016/j.chb.2012.11.022

Tang, J., & Lin, Y. (2017). Websites, data types and information privacy concerns: A contingency model. *Telematics and Informatics*, 34(7), 1274-1284. doi:10.1016/j.tele.2017.05.012

Tavani, H. T. (2007). Philosophical theories of privacy: Implications for an adequate online privacy policy. *Metaphilosophy*, 38(1), 1-22. doi:10.1111/j.1467-9973.2006.00474.x

Thielman, S. (2016). Facebook recrafts 'like' button with Reactions, complete with an angry face. Retrieved July 6, 2019, from https://www.theguardian.com/technology/2016/feb/24/facebook-reactions-like-button-angry-love-haha-wow-sad-faces-heart.

Tufekci, Z. (2008). Can you see me now? Audience and disclosure regulation in online social network sites. *Bulletin of Science, Technology & Society*, 28(1), 20-36. doi:10.1177/0270467607311484

Turow, J., Hennessy, M., Draper, N. (2015). The Tradeoff Fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. *SSRN Electronic Journal.* doi:10.2139/ssrn.2820060

Turow, J. (2011). The daily you: How the new advertising industry is defining your identity and your worth. New Haven: Yale University Press.

Turow, J. (2003). Americans Online Privacy: The System Is Broken. Retrieved from http://repository.upenn.edu/cgi/viewcontent.cgi?article=1411&context=asc_paper

Van den Broeck, E., Poels, K., & Walrave, M. (2015). Older and wiser? Facebook use, privacy concern, and privacy protection in the life stages of emerging, young, and middle adulthood. *Social Media + Society*, 1(2), 205630511561614. doi:10.1177/2056305115616149

Viseu, A., Clement, A., & Aspinall, J. (2004). Situating privacy online: Complex perceptions and everyday practices. *Information, Communication & Society*, 7(1), 92-114. doi:10.1080/1369118042000208924

Wang, H., Zhang, R., & Wellman, B. (2018). Are older adults networked individuals? insights from east yorkers' network structure, relational autonomy, and digital media use. *Information Communication & Society*, 21(5), 681-696. doi:10.1080/1369118X.2018.1428659

Westin, A. F. (1967). *Privacy and freedom* ([1st]. ed.). New York: Atheneum.

Westin, A. F., Louis Harris and Associates, & Equifax Canada, I. (1992). The Equifax Canada report on consumers and privacy in the information age: Executive summary. New York, NY: Louis Harris and Associates.

Wellman, B. (1978). The community question: The intimate networks of East Yorkers. *American Journal of Sociology*, 84(5), 1201-1231. doi:10.1086/226906

Wellman, B. (1993). An egocentric network tale: Comment on Bien et al. (1991). *Social Networks*, 15(4), 423-436. doi:10.1016/0378-8733(93)90015-d

Wellman, B., Hogan, B., Berg, K., Boase, J., Carrasco, J.-A., Côté, R., Tran, P. (2006). Connected Lives: The Project1. In P. Purcell (Ed.), *Networked Neighbourhoods: The Connected Community in Context* (pp. 161–216). London: Springer London. https://doi.org/10.1007/1-84628-601-8_8

Wellman, B., Quan-Haase, A., & Harper, G. M. (2019). How do networked, connected, and socially limited individuals use digital media? A life course perspective. *Network Science*, 8(1).

Wellman, B., & Wortley, S. (1990). Different strokes from different folks: Community ties and social support. *American Journal of Sociology*, 96(3), 558-588. doi:10.1086/229572

Windschitl, M., & Sahl, K. (2002). Tracing teachers' use of technology in a laptop computer school: The interplay of teacher beliefs, social dynamics, and institutional culture. *American Educational Research Journal*, 39(1), 165-205. doi:10.3102/00028312039001165

Woo, J. (2006). The right not to be identified: Privacy and anonymity in the interactive media environment. *New Media & Society*, 8(6), 949-967. doi:10.1177/1461444806069650

Wood, M. (2019). Tech, data, privacy and time: It's a trade-off, but are we trading too much? Retrieved from https://www.marketplace.org/2018/07/23/tech-data-privacy-and-time-its-trade-are-we-trading-too-much/

Young, A. L., & Quan-Haase, A. (2013). PRIVACY PROTECTION STRATEGIES ON FACEBOOK: The internet privacy paradox revisited. *Information, Communication & Society*, 16(4), 479-500. doi:10.1080/1369118X.2013.777757

Zickuhr, K., & Madden, M. (2012). *Older adults and internet use.* Pew Research Center. http://www.pewinternet.org/files/oldmedia/Files/Reports/2012/PIP_Older_adults_and_internet_use/ Accessed 16 August 2018

Zonneveld, M., Patomella, A., Asaba, E., & Guidetti, S. (2019). The use of information and communication technology in healthcare to improve participation in everyday life: A scoping review. *Disability and Rehabilitation*, 1-8. doi:10.1080/09638288.2019.1592246

Zuboff, S. (2019). The age of surveillance capitalism : the fight for a human future at the new frontier of power / Shoshana Zuboff. (First edition.). New York: PublicAffairs.

Zuboff, S. (2019). Surveillance Capitalism and the Challenge of Collective Action. New Labor Forum, 28(1), 10–29. https://doi.org/10.1177/1095796018819461

Zukowski, T., & Brown, I. (2007). Examining the influence of demographic factors on internet users' information privacy concerns. 226 197-204. doi:10.1145/1292491.1292514

Appendices

Appendix A: Interview Questions

Interview Questions

Question 1) In what year were you born?
Question 2) Where were you born?
- **Question a.** Where else have you lived?
- **Question b.** How long have you lived in Toronto?
- **Question c.** In what year did you begin living at this address?

Question 3) What languages do you speak most often at home?
Question 4) What is your highest level completed schooling?
- **Question a.** Are you currently a student?
- **Question i.** *If yes:* are you a full or part time student?

Question 5) Who else lives here with you?
Question 6) Do you have a partner?
- **Question a.** *If partnered:* Are you married?

Question 7) Do you have children under the age of 18?
Question 8) What kinds of devices do you have? For example, desktop computers, tablets, laptop computers, cell phones, home phones or TV's.
- **Question a.** Do you share any of these?
- **Question i.** If yes: Why do you share these devices and with whom?
- **Question ii.** If no: Why don't share your devices?

Question 9) Do you pay for cable or satellite TV services such as those offered by Bell or Rogers?
- **Question a.** *If no:* Do you use an antenna?

Question 10) Do you have a device to connect your TV to the internet?
- **Question a.** *If yes:* What do you use?

Question 11) Do you ever watch TV shows or movies online?
Question 12) Do you ever watch TV or movies on your mobile device(s)?
Question 13) Some people use more than one device at the same time, such as using their cell phone while on the computer. Do you ever find yourself doing this?
- **Question a.** What sorts of things do you do?

Question 14) Do you ever do any of the following, at least once per week, while watching TV or video content?
- **Question a.** Browse the internet
- **Question b.** Use social forums (such as Facebook, Twitter)
- **Question c.** Chat (using, for example, MSN, Skype, Facebook chat)
- **Question d.** Is there anything else you do while watching TV or video content?

Question 15) Do you ever go online to discuss a TV show or a video while watching it?
Question 16) What kind of cell phone do you have?
- **Question a.** Is it an ordinary cell phone or a smart phone, such as an iPhone, android or Blackberry?

Question 17) What do you use your cell phone for?
- **Question a.** *If they have a smartphone:* Do you have a data plan?
- **Question b.** *If they have a smartphone and if yes:* What do you do online from your phone?

Question 18) What do you use it for? (e.g. Notes, Facebook, Music, Phone, Text, Games, Surf, Reading, Picture taking, watching TV)
Question 19) Do you know how to download a file from the internet to your computer?
Question 20) Do you know how to send a file that is on your computer's hard drive to someone else?
Question 21) What search engines do you know?
Question 22) In terms of your internet skills, do you consider yourself to be not at all skilled, not very skilled, fairly skilled, very skilled or expert?
- **Question a.** How do you think your skills compare to those of your friends and relatives?
  - **Question i.** *If better:* Why do you think they are more skilled?
  - **Question ii.** *If worse:* Why do you think you are more skilled?

Interview Questions

Question 23) Out of all the devices you own, which are the most important to you?
- **Question a.** If you had to pick one, which would it be and why?

Question 24) Are there things you used to do with a computer that you now mostly do on your mobile phone or tablet? (For example, writing a long email, editing a paper, or watching a movie?)

Question 25) Are there things you used to do on your cell phone or tablet that you now mostly do on your computer? (For example, writing a long email, editing a paper, or watching a movie?)

Question 26) Suppose you were moving or you knew a hurricane was coming, what things would you find most important to preserve? (For example, photos, birth certificates, CD's, souvenirs, electronics, or vehicles?)

Question 27) What about the internet? What online things would you want to preserve for your family? (For example, your Facebook page, diary, photos, financial records, emails, or work documents?)

Question 28) Are there any things you physically have that you would rather keep in digital form on your computer or on the internet? (For example records, e-books, photos, government, or financial documents?)

Question 29) If you were very busy and someone sent you a message or called, would you answer immediately or wait until you are free?
- **Question a.** Why?
- **Question b.** Would this change if it were a family member, friend, partner or boss?

Question 30) If you needed to contact someone what would you do?
- **Question a.** What if you couldn't reach them right away?

Question 31) Does where you are change the ways you communicate?
- **Question a.** How so?

Question 32) When you are able to use a home phone, internet phone (such as Skype) or a cell phone, which do you choose and why?
- **Question a.** If the person you are contacting has both a home phone and a cell phone, which number do you call?

Question 33) Do people expect you to be reachable at all times?
- **Question a.** *If yes:* How do you feel about that?
- **Question b.** Have you ever missed out on an opportunity because you could not be contacted?
  - **Question i.** *If yes:* Could you tell us more about this?

Question 34) Do you post on walls publicly on Facebook, email multiple recipients or use online discussion forums to reach multiple people at the same time?
- **Question a.** Why?

Question 35) How do you let others know of your availability? For example, do you share an online calendar, use social media, or get in touch with people directly?
- **Question a.** Could you tell us more about why you do it this way?

Question 36) Do people have to contact you directly to know where you are or do you ever share your location information with others online or through applications like 4 square or Facebook?
- **Question a.** Could you give us examples?

Question 37) How have any of these devices made a difference in your social life?

Question 38) Is there anything else you'd like to tell us about this or anything else you think we've missed?

Question 39) What do you do for a living?

Question 40) Do you do any other paid work?

Question 41) Are you self-employed?

Question 42) *If retired or otherwise unemployed:* When was the last year you did any paid work?
- **Question a.** What work did you do?

Question 43) About how many hours do you work per week?

Question 44) What are the main things you do at work?

Interview Questions

Question 45) Some people do all or some of their paid work at home. Do you usually work any of your hours at home?
- **Question a.** *If so:* how many hours a week do you work from home?
- **Question b.** *If so:* What are your reasons for working from home?
- **Question c.** *If so:* Could you tell us a little bit about the work you do at home?

Question 46) Do you have a direct boss or manager, or do you work in a single group, in multiple teams, independently, or in some other arrangement?
- **Question a.** How is work delegated to you? (for example in meetings, by email or phone)
- **Question b.** Whom do you usually contact about your tasks at work?
- **Question c.** How do you communicate with coworkers?
- **Question d.** *If in groups or teams:* How is your work organized inside your group or team?
- **Question e.** *If in groups or teams:* How do you discuss your work with group or team members?

Question 47) Do you socialize with coworkers outside of work?
- **Question a.** Could you tell us a little bit about that?
  - **Question i.** What do you do?
  - **Question ii.** Where do you meet?
  - **Question iii.** How are these get-togethers organized?*(Who and what media)*

Question 48) Are your coworkers similar to you or different in terms of the languages they speak, their culture, where they live, their professions or personal interests?
- **Question a.** How so?

Question 49) How often do you see your partner?

Question 50) How do you get a hold of your partner?

Question 51) What sorts of activities do you do with your partner?
- **Question a.** Do the two of you get together as a couple with others?
  - **Question i.** *If yes:* Could you tell me a little about this?
  - **Question ii.** *If yes:* How are these get-togethers arranged? *(Prompt: Who and what media)*

Question 52) Is your partner similar to you or different in terms of the languages they speak, their culture, where they live, their profession or personal interests?
- **Question a.** How so?

Question 53) Who are you in frequent contact with?

Question 54) How do you contact them?
- **Question a.** Why do you choose this way?

Question 55) Do you usually see family members individually, or in groups?
- **Question a.** Why is that?
- **Question b.** How are these get-togethers organized? *(Prompt: Who and what media)*
- **Question c.** *If partnered/married:* Is this different for when you get together with your partner's family?
  - **Question i.** *If yes:* How so?

Question 56) Are your family and your partners family members similar to you or different in terms of the languages they speak, their culture, where they live, their professions or personal interests?
- **Question a.** How so?

Question 57) Do you ever socialize with them?
- **Question a.** *If yes:* In what way?
- **Question b.** *If* yes: How many neighbours do you frequently chat with?
- **Question c.** *If yes:* How many have you gone to visit at their homes or have come to visit you at home?
- **Question d.** *If yes:* Do you give each other any kind of help?
  - **Question i.** *If yes:* Could you tell me about it?

Interview Questions

Question e. *If yes:* Are your neighbours similar to you or different in terms of the languages they speak, their culture, where they live, their professions or personal interests?

Question i. How so?

Question 58) Are you a member of any church, sports, ethnic or cultural groups, charities or other voluntary groups?

Question a. *If yes:* Are you active?

Question b. *If yes:* Are you a leader?

Question c. *If yes*: Could you tell us more about what you do there?

Question 59) How do you communicate with those you volunteer with?

Question 60) Are the people you volunteer with similar to you or different in terms of the languages they speak, their culture, where they live, their professions or personal interests?

Question a. How so?

Question 61) Do you normally see your friends individually or do you tend to do things in groups?

Question a. Could you tell us more about this?

Question 62) What sort of things do you do together?

Question 63) Who organizes these things?

Question a. How are they usually organized, for example by phone, email or in person?

Question 64) Do you do things spontaneously with friends?

Question a. *If yes:* Could you give us some examples?

Question b. *If yes:* Does this happen often?

Question 65) Where do you meet with your friends in person?

Question a. Do you meet with your friends online?

Question i. *If so:* Where?

Question 66) Are your friends similar to you or different in terms of the languages they speak, their culture, where they live, their professions or personal interests?

Question a. How so?

Question 67) How do you and your friends communicate with one another? For example, do you use phone calls, texts, emails or Facebook updates?

Question a. Why do you think you choose this way?

Question 68) Are you connected in any other ways to any of the people we just discussed?

Question a. *If yes:* Could you give us an example?

Question 69) Have you ever introduced friends or acquaintances to one another?

Question a. *If yes:* why did you decide to do this?

Question b. *If yes:* How did it work out? Do they still see each other?

Question 70) Have you met anyone new, made any new friends, or reconnected with old friends lately?

Question a. *If yes:* How did this come about?

Question b. *If yes:* What drew you together? Why did you decide to become closer with this person again?

Question 71) If you wanted to, how would you go about making new friends?

Question a. Why would you go about it this way?

Question 72) Did you encounter a situation over the past year when you gave or needed help from someone? This could include finding a job, dealing with an illness, fixing a computer, emotional support, childcare, lending money, moving or finding a place

Question a. *If yes:* Could you tell us about that, if you feel comfortable doing so?

Question b. *If yes:* What kind of help was given?

Question 73) Do you think of yourself as a private person?

Question a. Why is that?

Question 74) How do you feel about organizations collecting information about you?

Question a. Do you take any steps to try to prevent this from happening? For example, refusing to use store point cards or shredding mail.

Interview Questions

Question b. Have you ever had an experience where you felt like your privacy had been compromised?

Question i. *If yes:* Could you tell me what happened?

Question 75) Do you have an account on any social media sites, such as Facebook, Twitter and LinkedIn? (If clarification is needed: on any sites where you can create an account and connect to other people's accounts in order to share information with each other?)

Question a. *If no:* Why is that?

Question b. *If no:* Do you ever use someone else's account to access things like pictures or posts?

Question c. *If yes:* What are your reasons for choosing to use Facebook, twitter or another social media service?

Question i. Which are most important to you?

Question ii. What do you usually use each of these sites for?

Question iii. What kinds of things do you post on these sites?

Question iv. Do you ever try to limit who can see what you post?

Question 1. Why do you do this?

Question 2. How? *(We're looking for what information they protect and who they keep it from, but technical details are okay too.)*

Question v. Is there any personal information you are uncomfortable posting online?

Question 1. *If yes:* What about it makes you uncomfortable?

Question vi. Are you ever concerned about what other people post about you on social media sites?

Question 1. *If yes:* What do you do about that? *(Looking for things like deleting posts, untagging pictures, etc.)*

Question vii. Have you ever had someone you didn't want to connect with try to connect with you on a social media site?

Question 1. *If yes:* How did you handle it?

Question viii. Have you ever decided to drop someone from your connections on a social media site, such as unfriending someone on Facebook?

Question 1. *If yes:* Why?

Question 76) Have you ever talked online to someone whom you didn't already know from somewhere else?

Question a. *If yes*: Have you ever had ongoing contact with someone you met online, or do you usually just talk to them once or twice? *(If there are multiple people, try to get a few examples in the following questions.)*

Question i. What did you talk about with them?

Question ii. *If there's ongoing contact:* How would you describe your relationship with them?

Question iii. Have you ever met anyone in person after first encountering them online?

Question b. *If no:* Is there a reason you don't talk to new people online? *(Probe for reasons related to 1) no desire/interest; 2) no opportunity; 3) privacy concerns.)*

Question 77) Do you generally use your real name when communicating on the internet, or do you sometimes use alternate names, like fake names or nicknames?

Question a. *If both:*

Question i. How do you decide which to use when?

Question b. *If sometimes:*

Question i. How do you pick your alternate name(s)?

Question ii. Do you use the same alternate name on different sites?

Question 1. Could you tell me about that?

Question iii. When you're using an alternate name, have you ever revealed your real name?

Question 1. *If yes:* Could you tell me about that?

Interview Questions

Question 78) Have you ever decided not to join a web site or use an online service because you felt they wanted too much personal information?

Question a. *If yes:* Could you tell me about a specific example?

Question 79) When using the internet, have you ever been concerned that you might have given out too much personal information or felt like your privacy or safety were at risk?

Question a. *If yes:* Could you tell me about that, what was your biggest concern?

Question b. *If yes:* Did this experience change how you give out personal information online?

Question c. *If no:* Have you heard of anyone else who had a negative experience?

(Probe: If they ask for clarification give the following examples: 1) "identity theft"; 2) having others see personal information out-of-context; 3) potentially embarrassing pictures being posted online without permission.)

Question i. Could you tell me what happened?

Question ii. Did this story change anything about the way you use the internet?

Question 80) Do you do anything else to try to protect your privacy when you're using the internet? *(Probe: If they ask for clarification, this could include government, corporations, future employers, colleagues and/or parents.)*

Question a. *If yes:* What kinds of things do you do?

Question b. Are there any people or types of organizations you'd rather didn't access some of your personal information?

Question i. Why is that?

Question 81) Do people you know seem concerned about the internet and privacy?

Question a. *If yes:* Could you tell me about their concerns?

Question b. *If no:* Why do you think that is?

Question 82) Have you shared any photos or videos of your kids with friends or family members through email or by putting them up online somewhere?

Question a. *If no:* Why not?

Question b. *If yes:* What kinds of things do you put up?

Question c. *If yes:* how do you decide if you should share this information publicly, for example on a Facebook wall or public photo sharing site, or privately, such as through email?

Question d. *If yes:* Do you ever try to limit who can see what you post about your children?

Question 83) Do you and your child do anything together on the internet?

(Probe: For example, gaming, looking at videos, searching for information or updating Facebook.)

Question 84) Do you ever worry about your children's privacy or safety when they're using the internet?

Question a. *If yes:* What are your main concerns?

Question i. What do you do about it?

Question b. Have any of your children ever had a negative experience when using the internet?

Question i. *If yes:* Could you tell me about what happened?

Question ii. *If no:* Do you know of anyone else's child who had a negative experience when using the internet?

Question 1. Could you tell me about it?

Question 85) Have you received information about how to help keep your kids safe and protect their privacy when they're on the internet?

Question a. *If yes:* Where did you get this information?

Question b. *If yes:* Was this helpful?

Question 86) Regarding the risks for kids when using the internet, what kind of information do you wish you had more of?

Question 87) Is there anything else that you would like to add?

Question 88) If we have some more questions, may we call on you again?

Curriculum Vitae

Name:	Kaitlyn Cavacas
Post-secondary Education and Degrees:	University of Windsor Windsor, Ontario, Canada 2019-Present M.S.W. Western University London, Ontario, Canada 2017-2019 M.A. Sociology Western University London, Ontario, Canada 2011-2016 B.A. (Hons) Sociology, Minor in Philosophy
Honors and Awards:	Western Graduate Research Scholarship 2017-2018, 2018-2019
Related Work Experience	Teaching Assistant Western University 2017-2019 Course: *Sociology 2140 Social Problems* Course: *Sociology 2172 Sociology of Advertising* Teaching Assistant Kings University College at Western University 2017-2018 Course: *Sociology 3361 Crimes of the Powerful* Teaching Assistant Kings University College at Western University 2018-2019 Course: *Sociology 2266 Introduction to Criminology*